

Brussels, 2 October 2026
(OR. en)

13928/26

Interinstitutional File:
2026/0301 (COD)

JAI 1239
SCHENGEN 29
ENFOPOL 359
ENFOCUSTOM 115
CYBER 397
CODEC 1828
CADREFIN 417
IA 254
PROCIV 190
TELECOM 464

PROPOSAL

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	1 October 2026
To:	Ms Thérèse BLANCHET, Secretary-General of the Council of the European Union
No. Cion doc.:	COM(2026) 1010 final
Subject:	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing the European Union Critical Communication System (EUCCS)

Delegations will find attached document COM(2026) 1010 final.

Encl.: COM(2026) 1010 final



EUROPEAN
COMMISSION

Brussels, 30.9.2026
COM(2026) 1010 final

2026/0301 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

establishing the European Union Critical Communication System (EUCCS)

{SEC(2026) 1010 final} - {SWD(2026) 1010 final} - {SWD(2026) 1011 final}

CONTEXT OF THE PROPOSAL

• Reasons for and objectives of the proposal

In any emergency situation, from floods and earthquakes to terrorist attacks, fires and traffic accidents, people rely on first responders and emergency services, such as law enforcement, rescue and medical services, and firefighters, for help. To provide help effectively, these first responders and emergency services need to be able to communicate and coordinate. Each Member State therefore provides dedicated, non-public, and secure communications systems for its emergency services (“critical communications systems”). These are mobile radio communication systems used by emergency services¹ that meet specific requirements in terms of reliability, security and availability. These systems are built to withstand disruption and continue to operate even when other communication channels fail. They are crucial for coordinating the response to emergency and crises and thus ultimately help save lives.

However, these national systems reach their limits when first responders cross borders or when they need to communicate with first responders from another Member State. Emergencies, especially major emergencies, often affect several Member States or require support from services from other Member State. An effective response to such emergencies, as well as the daily protection of citizens across the Union and the Schengen area, require that emergency services can *cooperate* with each other whenever and wherever they are, and can communicate seamlessly across the EU. Yet today, there is no European system that allows critical cross-border communication. This can complicate and delay the response in scenarios like joint police patrols, hot pursuits across borders, as well as accidents or major disasters such as fire or flood. In all these scenarios, most emergency services in Europe must rely on ad-hoc arrangements, such as the physical exchange of radios, creating a patchwork of different communication solutions or using commercial phones that are neither designed nor equipped for public security and safety tasks. Efficient and seamless communication is however not a matter of convenience: the ability to communicate defines the speed in which emergency services can react. And that in turn defines how fast they can save lives.

The European Union Critical Communication System (EUCCS) aims to provide a European solution, to equip those who protect us with the best communication means to fulfil their mission. EUCCS will serve more than 5 million first responders in emergency services² across Europe in their daily life-saving operations and during major emergencies. It will significantly increase Europe’s response capability both in times of large-scale crises, but also in daily emergencies, accidents, missing persons, crime and terrorism.

The 2015-16 wave of terrorist attacks, which brought to light the lack of communication among emergency services in major crisis situations, showed the clear need for greater

¹ ‘Emergency service’ means a service, recognised as such by the Member State, that provides immediate and rapid assistance in situations where there is, in particular, a direct risk to life or limb, to individual or public health or safety, to private or public property, or to the environment, in accordance with national law. <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32018L1972>.

² The figure represents the number of expected users of EUCCS, as communicated by Member States. this is not the number of interventions, but of *personnel* that uses critical communication means, and thus will benefit directly from EUCCS. The number is based on a questionnaire to Member States’ competent authorities in which they were asked for report the expected number of users (such as police officers, firefighters, medical services) to DG HOME.

interconnectivity and interoperability of critical communications. This need led to the launch of technical and operational coordination projects that prepared the EUCCS. The Covid-19 Pandemic, large-scale natural disasters such as wildfires, as well as the Russian war of aggression against Ukraine further highlighted the importance of improved critical communication capabilities, across different sectors. The initiative thus builds on, and is part of, a long-term and strategic approach that is based on concrete operational needs.

EUCCS directly addresses the operational needs expressed by Member States and emergency responders. Building on the results of EU-funded security research projects carried out in 2016-2023 - with involvement of first responders - the Commission is currently developing with Member States the technical framework for EUCCS. In 2023, DG HOME established the Mission Critical Communication Group (MCCG), comprising experts in the field of critical communication from the EU Member States, the Schengen Associated countries, and EU Agencies. This demonstrates the strong involvement of Member States, who had specifically requested leadership by the Commission on EUCCS with the common understanding that only EU-level action would be able to deliver such an ambitious system.

The legal framework presented in this Regulation is a light regulatory approach with a minimum set of binding rules at EU level. This solution responds best to the complex technological, operational, legal and political needs of the initiative. EUCCS creates a ‘system of systems’ in which Member States remain in full control of their critical communication systems, with mandatory inter-operability. At the EU-level, there would be no central data management infrastructure. Rather, a technical interconnection infrastructure overseen by a light governance component consisting of national Competent Authorities represented in a European Union Critical Communication Group would provide the basis for interoperability, as well as common support functions for Member States’ systems and operations. The system is planned to be built in a gradual approach, taking into account the different stages of transition to broadband communication of Member States’ national critical communication systems. A first group of Member States should start operations in 2030, followed by the other Member States in 2033 and 2036, the latter being the final deadline by which all Member States must connect to the EUCCS. This flexibility allows Member States to adapt their adherence to the EUCCS to the progress at national level, while already providing the full benefits of the interoperability to those Member States that are ready earlier.

The system will cover the whole EU and – in view of the need and benefit of including the full Schengen area – also the Schengen Associated Countries. For EUCCS to unfold its full added value and to allow comprehensive communication and coordination in case of major emergencies, it is essential that it covers *all* emergency services: law enforcement, firefighters³, civil protection and medical emergency responders. This proposal is therefore intrinsically linked with the proposal for a Regulation establishing the framework for the use

³ In line with the importance of tools in terms of connectivity, communication and coordination like the European firefighting hub based in Cyprus announced by the President of the European Commission in State of the Union Address 2025.

of the European Union Critical Communication System by the Member States' services and other organisations in charge of civil protection.

- **Consistency with existing provisions in the policy area**

In the field of critical communication, an EU acquis does not yet exist. Member States' critical communication systems are operating independently without legal harmonisation and with limited interoperability.

- **Consistency with other Union policies**

The proposed Regulation establishes the legal basis for the EUCCS in line with the provisions laid down in accordance with the existing and proposed legal acts in the area of civil protection, space and defence, cybersecurity, digital innovation and infrastructure and connectivity, including spectrum related aspects. Specifically, the Union Civil Protection Mechanism⁴ establishes operational cooperation between Member States in emergency response. The 112 and eCall provisions as part of the European Electronic Communications Code⁵ and the Digital Networks Act⁶ regulate the electronic communications sector. Regarding mobile satellite systems (MSS) management it takes into account the recently proposed MSS Regulation⁷. For what concerns coverage and backup, the proposed EUCCS regulation is in line with the Space Programme, in particular its secure connectivity component. Finally, it is coherent with the Network and Information Security 2 (NIS2)⁸ and Critical Entities Resilience (CER)⁹ Directives. The proposed Regulation complements the regulatory landscape by determining resilience requirements for Member States' critical communication systems that are aligned with NIS-2 and CER, as well as the Cyber Resilience Act to be fully applicable as of 11 December 2027.

The proposal is consistent with the *Council Conclusions of 7 June 2021 on the protection of public spaces*¹⁰, which emphasised the importance of secure, interoperable mission-critical communication. The *EU Space Strategy for Security and Defence*¹¹ was the first European Commission document to identify the creation of a European Union Critical Communication System as a policy objective.¹² In 2024, the political commitment was confirmed in the

⁴ Proposal for a Regulation of the European Parliament and of the Council on the Union Civil Protection Mechanism and Union support for health emergency preparedness and response, and repealing Decision No 1313/2013/EU (Union Civil Protection Mechanism) COM(2025) 548 final.

⁵ Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code.

⁶ Proposal for a Regulation of the European Parliament and of the Council on digital networks, amending Regulation (EU) 2015/2120, Directive 2002/58/EC and Decision No 676/2002/EC and repealing Regulation (EU) 2018/1971, Directive (EU) 2018/1972 and Decision No 243/2012/EU (Digital Networks Act) COM(2026) 16 final.

⁷ Proposal for a Regulation of the European Parliament and of the Council on the procedure for authorisation of systems providing mobile satellite services using the harmonised 2 GHz frequency band and repealing Decision No 626/2008/EC. COM(2026) 0134 final.

⁸ <https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng>

⁹ <https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng>

¹⁰ [Council Conclusions 9545/21 on the Protection of Public Spaces \(2021\); Council Recommendation \(EU\) 2022/915 on operational law enforcement cooperation \(2022\);](#)

¹¹ [https://ec.europa.eu/transparency/documents-register/detail?ref=JOIN\(2023\)9&lang=en](https://ec.europa.eu/transparency/documents-register/detail?ref=JOIN(2023)9&lang=en)

¹² https://defence-industry-space.ec.europa.eu/eu-space/eu-space-strategy-security-and-defence_en.

Commission White Paper ‘How to master Europe’s digital infrastructure needs’, which announced the establishment of EUCCS by 2030.¹³ Further momentum came with the *2024–2029 Political Guidelines* of Commission President von der Leyen, which stated that “*our united approach to security should be centred around a new European Critical Communication System (...)*”. The Niinistö Report¹⁴ also urged the EU to complete the EUCCS as soon as possible and recommended to ensure its interoperability with systems used by armed forces. This direction was reaffirmed in 2025 in *ProtectEU – the European Internal Security Strategy*¹⁵ and the *European Preparedness Union Strategy*¹⁶, both announcing a legislative initiative. The Preparedness Union Strategy specifically highlights the effects of recent crises on multiple sectors and promotes a whole-of-government approach, bringing together all relevant actors, across all levels of government, ensuring collaboration and sharing of resources, to which the EUCCS would contribute.

1. LEGAL BASIS, SUBSIDIARITY AND PROPORTIONALITY

• Legal basis

The legal basis is Article 87(2)(a) of the Treaty of the Functioning of the European Union. Article 87(1) of the Treaty of the European Union lays down the legal basis for the establishment of police cooperation, including police, customs and other specialized law enforcement services in relation to prevention, detection and investigation of criminal offences. In this regard, Article 87(2)(a) of the Treaty of the Functioning of the European Union provides for the possibility to establish measures concerning the collection, storage, processing, analysis and exchange of relevant information. This includes the development of necessary technical infrastructure.

Article 87(2)(a) of the Treaty of the Functioning of the European Union is the appropriate legal basis for the establishment of the European Union Critical Communication System for law enforcement authorities across borders among Member States and Schengen Associated Countries. This regulation constitutes further development of the Schengen acquis, as it further develops the Decision of the Executive Committee of 28 April 1999 on the Schengen acquis relating to telecommunications.

• Subsidiarity

This proposal responds to calls from Member States and first responders for action at EU level to facilitate and establish a legal framework for broader critical communication among Member States as system of systems. The proposal aims to create a Union-wide interoperable communication system for first responders by interconnecting the national systems, ensuring seamless coordination during emergencies across Member States.

¹³ European Commission, *White Paper: How to Master Europe’s Digital Infrastructure Needs* (2024) <https://digital-strategy.ec.europa.eu/en/library/white-paper-how-master-europes-digital-infrastructure-needs>.

¹⁴ Niinistö, S. (2024), *Safer Together – Strengthening Europe’s Civilian and Military Preparedness and Readiness*, p. 59 and p. 69.

¹⁵ COM (2025)148final (2025) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025DC0148>.

¹⁶ European Commission (2025), *European Preparedness Union Strategy*, [JOIN\(2025\) 130 final](#).

Given the transnational nature of the European Union Critical Communication System, including standardisation, interoperability and cross-border cooperation among first responders, EU action is necessary.

National rules are insufficient to guarantee the required interoperability, responsibility, and resilience of the communication system as they cannot create the necessary binding EU-wide interoperability framework. The measures set out in this proposal must be adopted at Union level to achieve the intended cross-border objective of establishing the European Union Critical Communication System. Therefore, Union action is justified under the principle of subsidiarity.

• **Proportionality**

The proposal lays down rules for Member States and providers of publicly available interpersonal communications services for the establishment of an effective, secure and interoperable critical communication system. The proposal defines clear rules for Member States to develop the required architecture and infrastructure for the EUCCS, including minimum resilience and security standards. These technical and operational demands are strictly limited to what is essential to ensure that the EUCCS functions as a cohesive and secure network system, capable of supporting cross-border communication among public security authorities. The interconnectivity between current communication networks enhances the systems' efficiency and operational readiness, ensuring that first responders and emergency services can rely on secure communication channels during critical operations.

The proposal takes into account that a system of systems solution imposes requirements on Member States and service providers in order to establish a decentralised EU framework that allows the national critical communication systems to be interconnected. It creates a framework for Member States to designate competent national authorities that are obliged to ensure the interconnectivity of Member States' critical communication systems. The chosen form of a decentralised EU framework - i.e. without a central EU competent authority - balances the necessary requirements to establish a functioning EU and Schengen wide interoperable communication system and the respect for national autonomy, without imposing excessive requirements on the Member States. This architecture ensures that the EUCCS functions as a unified framework to enhance overall effectiveness.

The proposal also requires Member States to impose rules on telecommunications service providers to ensure the use of their networks for critical communication. These requirements ensure that existing infrastructure can support the operational needs of the EUCCS, without placing disproportionate technical or financial demands on service providers.

The measures taken are limited to responding to the essential needs for the creation of a resilient and secure cross-border critical communication system between Member States and security agencies.

• **Choice of the instrument**

Given the nature of emergency services, which bring together several different authorities and services from Member States, the EUCCS consists of two proposals relying on two different legal bases to ensure comprehensive interoperability across all relevant services. The first –

present – proposal is based on Article 87 (2) (a) of the Treaty on the Functioning of the European Union (TFEU), which gives the European Parliament and the Council, acting in accordance with the ordinary legislative procedure, the possibility to establish directives and regulations to facilitate police cooperation.

To include all relevant emergency services in the EUCCS, the scope of the framework is extended to civil protection services and other organisations in charge of public safety by a second regulation, Regulation EU (.../...) on establishing the framework for the inclusion of the Member States' civil protection services and other organisations in charge of public safety into the European Union Critical Communication System, which is proposed in parallel and is based on Article 196 TFEU.

Given the need to ensure a light central governance structure and one clear and unified interoperability framework interconnecting the national systems, a regulation is the appropriate legal instrument.

The proposal aims to establish a Union-wide critical communication system across Member States and Schengen associated countries, ensuring secure and interoperable cross-border communication for public authorities. A regulation is necessary to achieve direct application across all Member States, thereby guaranteeing consistent implementation without the risk of divergent national approaches that could compromise interoperability. This also ensures the system can be operational without delay, addressing urgent security needs effectively. A regulation is the only suitable legal instrument for establishing the binding technical specifications, security standards, and governance structures required to support such a system.

2. RESULTS OF EX-POST EVALUATIONS, STAKEHOLDER CONSULTATIONS AND IMPACT ASSESSMENTS

• Ex-post evaluations/fitness checks of existing legislation

As the Regulation relates to a new area with no existing legislation at EU level, this point does not apply.

• Stakeholder consultations

The Commission collected data through various sources and consultations methods.

The EUCCS system is built in close cooperation with the European industry, therefore directly contributing to the overarching priorities of strategic autonomy and competitiveness. In compliance with the Better Regulation guidelines, DG HOME published a Call for Evidence in April 2025 and commissioned an external study to support the Impact Assessment. The research for the initiative and this impact assessment started with targeted surveys and interviews with EU Member States, which took place from July 2025 until June 2026 and mapped how Member States authorities are currently implementing their critical communications system.

A Commission Open Public Consultation was conducted from 16 January until 10 April 2026. Commission services also conducted targeted surveys and organised dedicated meetings with representatives of industry, such as providers of critical communication infrastructure and

services and mobile network operators, as well as NGOs and other relevant associations, which took place from July 2025 until June 2026.

• **Collection and use of expertise**

As mentioned in the preceding section, the Commission has drawn on external expertise in the context of consultations with, e.g. independent experts, expert networks and members of academia, in developing the proposal at hand.

• **Impact assessment**

This proposal is supported by an impact assessment, which analysed a range of policy options to address the identified problems related to limited operational mobility, limited functionality of legacy systems and insufficient resilience.

The general objective of EUCCS is to enhance Europe's capacity to react swiftly and effectively to incidents and crises that require response across borders and by cooperation of different types of emergency services.

Three specific objectives have been identified as:

- Specific Objective no. 1: Promote interoperable and secure cross-border and cross-agency/operator critical communication and operational mobility among emergency services

The objective is to provide emergency services with a resilient critical communication infrastructure. The system should enable seamless operational mobility, meaning the ability of emergency services to communicate seamlessly whenever, wherever and with whomever they are tasked to cooperate. It shall furthermore promote interoperability and strengthen cross-border and cross-agency operational mobility for an enhanced emergency response. Specifically, all the critical communication systems of law enforcement, civil protection, and other emergency response services across Member States need to be harmonised and interconnected.

- Specific Objective no. 2: Support Member States in deploying broadband critical communication systems

The ability to exchange data-rich information, such as images or video, across borders and in real time is a key driver behind Member States' decision to upgrade the current narrowband systems used, notably TETRA¹⁷. It is important to underline that EUCCS does not 'replace' TETRA. Rather, it is the technological shift to broadband that will phase out narrowband technologies, similar to what happened in commercial telecommunication.

The transition to broadband is necessary for the deployment of interoperable 5G mission-critical capabilities. Broadband communications technology satisfies the current and evolving needs for increasing data consumption, supporting advanced functionalities, such as real time incident reporting and facilitating the integration of Artificial Intelligence. Furthermore, technological harmonisation will contribute to making national investment in critical

¹⁷ TETRA, or Terrestrial Trunked Radio is a global standard for digital radio technology. In contrast, Tetrapol is a 1988 proprietary technology even if its specification is publicly available.

communications attractive and help build a more integrated and technologically advanced European critical communications ecosystem.

- Specific Objective no. 3: Facilitate the achievement of a high and consistent level of resilience of critical communications across Member States

Resilient infrastructure is essential to ensure connectivity and availability in all circumstances. In this context, resilience refers to the capacity of critical communication infrastructures to withstand, absorb, and rapidly recover from natural hazards, man-made disasters or security incidents. Notably this can be achieved by ensuring advanced backup power, redundant coverage, the separation of mission critical core network and radio access networks, as well as strong protocol and cryptographic security. A broadband system would also contribute to a higher level of security by authentication allowing for stronger protection against cyberattacks. Furthermore, achieving this specific objective would contribute to future-proofing critical communication systems and increasing Europe's strategic autonomy against potential geopolitical developments harming EU interests.

On the basis of these objectives, the impact assessment that supported the development of this initiative explored different policy options. Besides the baseline situation, which would entail no change over the current situation, these options included:

- Policy Option 1: voluntary pursuit of technical interconnectivity

This policy option is based on voluntary measures to promote interconnection of critical communication systems between Member States. This would include the publication of non-binding guidance by the Commission. Similarly to the baseline scenario, Member States would continue to develop their national critical communication systems independently. They would either maintain narrowband systems or transition to broadband solutions, in line with national strategies, priorities, and available resources.

In theory, PO1 addresses all problems and their drivers, however it is very unlikely to solve any of them in a satisfactory manner. Given the voluntary nature it is extremely unlikely that all Member States and all emergency services would participate in a 'voluntary EUCCS'. The consultation with Member States concluded that only eleven Member States would be willing to work on interoperability of broadband systems in the absence of a binding EU framework. The BroadMap and BroadWay projects (2016 – 2022) were based on a voluntary approach that should lead to a coordinated procurement of inter-operable solutions. Experience gained from those projects largely led to the common understanding of Member States and the Commission services that only an approach based on binding EU-level rules is likely to successfully establish EUCCS.

In PO1, the Mission Critical Communication Group would recommend relevant international standards (e.g. those developed by the European Telecommunications Standards Institute or 3GPP) and promote common operational procedures to support interconnection among participating Member States. EU funding of projects could be leveraged aligning to existing priorities.

- Policy Option 2: adoption of an EU legal act providing a legal basis for the establishment of a decentralised EU framework

This policy option would establish a ‘system of systems’ enabling the interconnection of Member States national critical communication systems while preserving Member States’ sovereignty over their national critical communication systems.

The legal act would set out objectives, roles and responsibilities, minimum technical requirements, and cross-border procedures. Implementation would take place gradually following a convergence period with an initial system connecting around eight to ten Member States by 2030, followed by a progressive expansion of services and participation in 2033 and 2036.

At the EU level, there would be no central data management infrastructure or central operations capacity but a governance, as well as common support functions for Member States’ systems. Interconnection of Member States’ systems will be facilitated, and a central EU level monitoring capacity will be established. The combination of those elements is the EU-level component of EUCCS. Two sub-options exist that differentiate from each other according to the level of centralisation of this EU-level component:

- In sub-option 2.1 the **EU-level component is light** with a stronger role of the Member States, for which the current EUCCS Preparation Project will be reinforced to become the EUCCS Cooperation Project and only the necessary elements for facilitating interconnectivity, monitoring and support tasks being handled at EU-level.
- In sub-option 2.2 a central **EU competent authority** covers tasks related to facilitation on technical interconnectivity, common EU services as well as monitoring of the implementation of EUCCS across Member States.

Policy Option 2.1 and Policy Option 2.2 present very similar benefits and impacts.

Policy Option 2.1 ensures a higher degree of coherence with existing EU policies and respects the principle of proportionality, as its measures are appropriately calibrated to the scale of the challenges addressed. The creation of the governance measures and the light EU component are relatively easy to achieve.

There is a variation of the cost, as Policy Option 2.2 requires slightly less human resources at EU level due to the centralised governance structure. However, Policy Option 2.2 would have required the creation of an EU Agency, or the significant modification of an existing Agency mandate and resources, to act as competent authority. The Commission has thoroughly reviewed existing Agencies and none of them would have the necessary legal mandate to cover the different first responder groups, as well as the resources and capacity to handle the EU component of EUCCS. Creating a new Agency on the other hand was determined to be disproportionate.

Considering these facts, Policy Option 2.1 emerges as the preferred option. This Policy Option provides the most effective response to the identified problem, offering a comprehensive and reliable framework for achieving the policy objectives. While it may entail higher costs compared to Policy Option 1, these are justified by the significantly greater benefits and the more substantial impacts generated across economic, social, and environmental dimensions. By contrast, Policy Option 1, although less burdensome, is not

expected to deliver sufficient impact to address the identified problems, limiting its overall suitability.

Different types of impacts have been identified and assessed in the Impact Assessment, including but not limited to:

- Social impacts: Significant and structural benefits through binding interoperability, harmonized procedures, and full operational mobility for an estimated 3.7 million first responders across the Union. Enhanced safety and security for citizens.
- Economic impacts: Substantial public investment (€3.571 billion) required for an interoperable EU-wide system. Medium- to long-term benefits include economies of scale, a more integrated market, and opportunities for European industry, particularly Small and Medium Enterprises (SMEs), in critical communication services, infrastructure, and equipment.
- Environmental impacts: More positive and structurally significant benefits through strengthened cross-border response capacity, enabling faster and more coordinated interventions to mitigate environmental risks.

EUCCS strengthens the capacity of emergency services and supports efficient coordination in emergency and crisis situations, accelerates response to disasters and emergencies, and enhances accountability and reliability. The general and specific objectives of the EUCCS contribute to various United Nations Sustainable Development Goals¹⁸, notably: SDG 11, SDG 13 and SDG 16.

The Impact Assessment was subject to scrutiny by the Regulatory Scrutiny Board, which issued a positive opinion with reservations on 22 May 2026. The Board suggested to identify better the collection of evidence presented; describe in more details the intervention logic and problem drivers, specifically what concerns the interoperability between Member States; elaborate in more detail the EU added value, preparedness of the Member States' technological solutions and future-proofness of the chosen policy option; and better clarify, assess and compare the costs and benefits of the options, including their distribution among the various stakeholders.

All these elements have been addressed in the final version of the Impact Assessment.

Lastly, the impact assessment explains that EUCCS will have positive impacts on the environment, notably as it enhances the capability to respond to disasters with environmental impacts such as floods, fires and industrial accidents, as well as the fight against environmental crime. Therefore, this legislative proposal is consistent with the climate-neutrality objective set out in European Climate Law.

The summary sheet of the impact assessment is available at the following link: [LINK to be inserted]

• Regulatory fitness and simplification

¹⁸ <https://sdgs.un.org/goals>

This initiative is not a revision of existing legislation; therefore, a REFIT test has not been performed.

• **Fundamental rights**

This proposal does not affect fundamental rights, but it supports Member States in the exercise of their responsibility to ensure the safety and security of their citizens. Specifically, the EUCCS enhances interoperability among emergency services across agencies and borders, ensuring an effective and coordinated response to security threats, crises, and the protection of citizens throughout the Member States. Member States' responsibility to ensure the security of every person is protected under Article 6 of the Charter of Fundamental Rights of the European Union (Charter), and Article 5 of the European Convention on Human Rights (ECHR). With respect to Article 2 ECHR and Articles 2(1) and 3(1) of the Charter, the EUCCS could support the protection of life as well as the physical and mental integrity of people by enabling rapid emergency response and coordination during crises such as terrorist attacks or natural disasters. EUCCS does not equip law enforcement and emergency services with any capabilities that may be used for direct exercise of force or infringements of other rights.

– Compliance with Regulation 2016/679 (GDPR Regulation)

The EUCCS fully comply with the standards laid down in Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR), in line with Article 8 ECHR (right to respect for private and family life), Article 7 (respect for private and family life) and Article 8 of the Charter (protection of personal data). The EUCCS facilitates the exchange of operational data exclusively among emergency services and directly associated entities, e.g. emergency medical services, hospitals. Such exchanges may include victim-related data, such as name, age, sex, physical or psychological condition, but remain strictly limited to public security and safety purposes. These advancements serve solely to improve emergency response, without altering the existing legal framework for data protection. The EUCCS not enhance the capabilities of law enforcement for activities with a potential fundamental rights impact, such as surveillance of private communication.

The restrictions of data subject rights (e.g. access, erasure, or objection) in cross-border data exchanges are in line with Article 23 GDPR, as the new dimension permits restrictions by way of a legislative measure when necessary for public security, national defence, or law enforcement, provided such limitations are proportionate. For critical communication, processing of personal data would be based on the vital interest to protect life and to prevent serious threats.

3. BUDGETARY IMPLICATIONS

The total costs have been established as part of the Impact Assessment in close cooperation with Member States' experts.

The total direct costs amount to €3,571 billion. Of those, for the EU component of the EUCCS, which is to be provided by the European Commission, the impact assessment

estimated the costs to amount to €1,156 billion, covering costs for the dedicated initial network connection, standardisation and certification, satellite connectivity, testbeds, the European Union Network Monitoring Centre, the European Union Security Monitoring Centre, the European Critical Communications Group Committee, the System Accreditation Board, the tasks of the EUCCS Cooperation mechanism, the elaboration of standard operating procedures and guidelines additional human resources and for training of staff.

The costs that are directly related to the establishment of the System at the level of the Member States and the interconnection of Member States' systems to jointly form the EUCCS amount to €2,415 billion, consisting of adjustment costs for network, infrastructure, user equipment, applications and software licences for connecting to the EUCCS, as well as of administrative costs, consisting of reporting tools for the national competent authority, human resources needed for reporting and statistical work, training.

The costs that Member States would have to cover for transiting critical communication to broadband over a period of 7 years are estimated at €12,667 billion, including the costs for using existing public networks. Those costs are not induced by the EUCCS.

Without prejudice to the outcome of the negotiations on the next Multiannual Financial Framework (MFF) the proposal, may be supported by Union programmes in accordance with the objectives set out in the regulations establishing those programmes. The LFDS presents estimated budgetary impact under Heading 4 including related human and administrative resources.

4. OTHER ELEMENTS

• Implementation plans and monitoring, evaluation and reporting arrangements

Key Performance Indicators (KPIs) will be used to measure the success of EUCCS, aligned with its specific objectives. These include: (i) the designation of National Competent Authorities (NCAs) and EU competent bodies; (ii) the establishment of the European Union Critical Communications Group (ECCG) and System Accreditation Board (SAB); (iii) the number of Member States connected to EUCCS and number of first responders with connectivity; (iv) the increased cross-border operational mobility (for instance, roaming minutes); (v) the service quality metrics (for example, connection time, roaming service quality, backup power capacity); (vi) compliance with security requirements (NIS2, Cybersecurity Act), using European cybersecurity certification schemes where available; (vii) the number of joint exercises and trained first responders; and (viii) progress in implementing national strategies and adherence to Standard Operating Procedures (SOPs).

The Commission will evaluate the functioning and effectiveness of the Regulation in line with standard evaluation requirements and report on its performance.

• Detailed explanation of the specific provisions of the proposal

The proposal is based on two Regulations as explained above. The main Regulation is based on Art. 87 TFEU and is structured as follows:

Chapter I – General Provisions

This chapter describes the subject matter and the scope, namely enabling emergency services and other public authorities in charge of security and public safety to seamlessly communicate and exchange mission-critical information with each other, across borders, thereby enhancing efficiency and effectiveness of response to emergencies and crisis situations. Furthermore, it provides the key definitions and sets out the obligation for Member States to ensure the interoperability of their national critical communication systems.

Chapter II – Member State Critical Communication Framework

This chapter describes the architecture of the Member States' Critical Communication Framework, which consists of the national critical communications system and the policies governing its upgrade and use, supervised by a national Competent Authority. Specifically, it describes the role of the Member State Competent Authority, the content of the national mission critical-broadband communication strategy, the minimum components, spectrum management and resilience requirements of the national critical communication system and the obligations for providers of public electronic communications networks. These rules ensure comparable frameworks and minimum harmonisation at Member State level, which is a prerequisite for a coordinated transition into mission critical broadband and the basis for the eventual interconnection of critical communication systems via the EUCCS. In line with the objective of technological sovereignty and with the Commission's Joint Communication on Strengthening EU economic security¹⁹, to lower the risk of data leakage, espionage and of physical and cyber-disruption, these rules exclude ownership, control or operation by high-risk entities and avoids dependencies on single suppliers or high-risk suppliers, as well as concealed vulnerabilities, backdoors or potential systemic ICT supply disruptions, by excluding high-risk vendors from the core of the system and thus contributing to ensure the supply chain security of the system.

Chapter III – European Union-level Governance

This chapter describes the governance at Union level. It sets out the European Union Critical Communication Group, consisting of Member States' delegates, that will steer policy implementation, as well as the System Accreditation Board which will perform the technical accreditation of Member States' critical communication systems to ensure readiness to join the EUCCS. A dedicated governance system ensures a strong role for Member States to safeguard their control over national systems, while providing clear and coherent guidance for the functioning of the EUCCS, as well as ensuring trust and verification of the accreditation, to support the future development of the System.

Chapter IV – System Accreditation and Interconnection

The chapter describes the steps for Member State systems' interconnection to form gradually the European Union Critical Communication System. It includes an empowerment for the

¹⁹ [JOIN/2025/977 final](#) of 3 December 2025.

Commission to adopt a delegated act to define the mandatory standards, explains the general principles of accreditation and interconnection and how the Commission will facilitate the interconnection via a dedicated infrastructure. Furthermore, it describes the principle of gradual establishment and the assessment missions to be performed before an accreditation to verify compliance with the legal obligations and technical standards. Due to the fact that Member States have different starting points and the transition into mission critical broadband will happen in different timelines and with different budgetary implications, a gradual approach is the only effective solution to ensure interconnection. The proposal sets 2036 as the final date for transition and interconnection. The provisions of this Chapter are supplemented by the Annex, which defines the Member States' maturity levels.

Chapter V – European Union Components

This chapter describes the European dimension of the light technical components of the System, namely the competences of the European Union Network monitoring centre and of the European Union Security Monitoring Centre. The Network Monitoring Centre would host the interconnection infrastructure and support the high-level monitoring of the functioning of the interconnection and the interoperability. The Security Monitoring Centre would support Member States' Security Operation Centres by monitoring security threats to critical communication systems. Both centres would be created as virtual service entities using framework contract arrangements of the European Commission that are already today used for similar tasks for the Commission and other EU bodies. Where relevant, both centres could be supported with advice from ENISA.

Chapter VI – Union-level operational support

This chapter describes the different European level operational support measures, namely the standard operating procedures and the use of EU Satellite Secure Connectivity services. Standard operating procedures are a key element to ensure that apart from the technical aspects, there is also operational harmonisation that is the basic for effective communication in emergency situations. EU Satellite Assets will support the System by offering Member States back-up and additional coverage where terrestrial systems are not available or disrupted. Finally, the chapter describes the supporting role of the Commission for Member States operations and system development, notably providing testbeds for the mission-critical interconnection, developing best practices, guidance materials and methodologies, and cross-border training activities and exercises to test critical communication systems for emergency services.

Chapter VII – Evaluation

This chapter defines the measures for evaluation of the Regulation.

Chapter VIII – Delegated and Implementing Acts

This chapter confers the power on the Commission to adopt delegated acts and specifies the committee procedure for the development of implementing acts.

Chapter IX – Final Provisions

This chapter lists the final provisions, notably that the Regulation would take immediate effect in all Member States.

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
establishing the European Union Critical Communication System (EUCCS)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 87 (2), point (a) thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee²⁰,

Having regard to the opinion of the Committee of the Regions²¹,

Acting in accordance with the ordinary legislative procedure,

Whereas:

- (1) People facing emergency situations in the Union depend on the fast, efficient, and professional response, including by law enforcement authorities. From daily operations, countering crime and terrorism, preserving the public order in case of incidents or attacks, or providing security for mass events, these services need to communicate seamlessly, exchange information in real time, and collaborate effectively between each other and across borders.
- (2) The effective functioning of the Schengen area and the prevention and response to security threats or disasters depend on close cross-border law enforcement cooperation, underpinned by continuous and reliable communication and information exchange in cross-border operations, such as hot pursuits. Law enforcement cooperation across borders within the area free of internal border controls on persons relies on the ability of competent public authorities to maintain reliable and interoperable communications when operating in a cross-border context, including in situations requiring real-time coordination. Such cooperation significantly contributes to ensuring the long-term security of the the Schengen area and of the Union citizens and, as such, constitutes an important safeguard in an area without internal border controls.
- (3) It is essential that public authorities in charge of ensuring public order and security have, within the framework of applicable Union and national law, the ability to communicate effectively both within and across borders. In such an area, law

²⁰ OJ C , , p. .

²¹ OJ C , , p. .

enforcement activities carried out by one Member State may have cross-border implications for the security of others, and effective cooperation increasingly depends on the capacity of authorities to coordinate actions and exchange information in a mission critical and reliable manner. Secure, resilient and interoperable critical communication systems therefore play a central role in ensuring continuity of law enforcement operations and missions across borders and constitute an essential component of the measures underpinning public security in an interdependent area without internal border controls. Critical communication infrastructure should guarantee the reliable, secure, and efficient transmission of vital information to respond, coordinate and cooperate.

- (4) At present, no system enables seamless cross-border cooperation between law enforcement authorities in the Schengen area. Critical communication systems of the Member States operate largely independently at national level and are based on differing technical approaches, resulting in very limited interoperability and lack of continuity of communications across internal borders. In an interdependent area without internal border controls, such fragmentation undermines effective law enforcement cooperation and the ability of authorities to respond jointly to security threats. It is therefore necessary to establish clear, harmonised and effective requirements at Union level, including common interoperability requirements and standards, to support the modernisation and interconnection of Member States' critical communication systems.
- (5) In order to address the need for operational mobility, strong resilience and strategic autonomy of the Member States' critical communication systems, the European Union Critical Communication System (EUCCS) should be established as an overarching framework that enables the relevant law enforcement authorities to communicate and exchange data continuously and seamlessly with corresponding authorities in other Member States for cross-border missions while operating within their familiar operational environments, including the devices, applications, authentication mechanisms and communication services they use in their routine activities.
- (6) The European Union Critical Communication System constitutes a key action at Union level in support of internal security objectives, as reflected in ProtectEU – the European Internal Security Strategy²², which emphasises the importance of enhanced cooperation, resilience and preparedness in addressing security threats to public order and security. Moreover, as highlighted in the European Preparedness Union Strategy²³, the Union should strengthen its response capabilities and strategic preparedness, including crisis-response tools, to address major emergencies, critical shortages and hybrid attacks. The establishment of a European Union Critical Communication System contributes to those objectives by providing a common framework enabling competent authorities in charge of security and safety to communicate and exchange data continuously and seamlessly.

²² <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52025DC0148>

²³ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025JC0130>

- (7) Whereas Member States may have different models for their national critical communication systems, a set of key minimum requirements and the ability of different types of law enforcement authorities to effectively communicate between each other within a given Member State is a prerequisite for interconnecting to the European Union Critical Communication System.
- (8) The critical communication framework established by this Regulation should be without prejudice to the organisation, command or conduct of law enforcement activities, or to the ownership and operation of national critical communication systems, which remain the responsibility of the Member States. The provisions laid down in this Regulation do not interfere with the competence of Member States and their authorities in terms of administrative autonomy. They do not affect their responsibility for safeguarding national security and defence, their power to safeguard other essential State functions, in particular concerning public security, territorial integrity and the maintenance of law and order.
- (9) In order for the European Union Critical Communication System to unfold its full operational value, Member States should be encouraged to ensure its use also by their services and other organisations in charge of civil protection, enabled by Regulation (EU) 2021/836 of the European Parliament and of the Council ²⁴. Cooperation between different types of emergency services is the daily operational reality. Law enforcement authorities depend on the seamless cooperation with firefighters, civil protection and medical emergency responders to effectively conduct its mission, thereby ensuring joint response of all relevant authorities in emergency situations.
- (10) There are other important users of critical communication systems. To cater for the different situations in Member States and to allow for flexibility, Member States should have at their discretion the to include other users into the System. This applies notably to armed forces, national security authorities, public authorities responsible for the protection of the environment and authorities or private entities responsible for the delivery of essential services, notably as provided in Commission Delegated Regulation (EU) 2023/2450²⁵ as well as for the operation of critical infrastructure as defined in national law. Private security operators, in particular Monitoring and Alarm Receiving Centres, play an essential role in the early detection and verification of incidents, including coordinated first response with competent authorities, affecting citizens, essential services, the resilience of critical entities, and public space security. They should therefore be recognised as trusted contributors to emergency response systems and consequently be included where appropriate in critical communication networks in a complementary role to emergency services and other public authorities.

²⁴ Regulation (EU) 2021/836 of the European Parliament and of the Council of 20 May 2021 amending Decision No 1313/2013/EU on a Union Civil Protection Mechanism (OJ L 185, 26.5.2021, p. 1, ELI: <http://data.europa.eu/eli/reg/2021/836/oj>)

²⁵ Commission Delegated Regulation (EU) 2023/2450 of 25 July 2023 supplementing Directive (EU) 2022/2557 of the European Parliament and of the Council by establishing a list of essential services (OJ L, 2023/2450, 30.10.2023, ELI: http://data.europa.eu/eli/reg_del/2023/2450/oj).

- (11) With a view to ensuring a comprehensive and harmonised approach to the transition towards critical broadband and the interconnection of Member States' systems into the European Union Critical Communication System, each Member State should have in place a strategy for critical communication. The strategy should set out objectives and policy measures to be implemented. In the interests of coherence and efficiency, the strategy should be designed to seamlessly integrate existing policies, building, wherever possible, upon relevant existing national and sectoral strategies, plans or similar documents.
- (12) Critical communication is increasingly shifting towards broadband, using commercial public electronic communications networks on a shared infrastructure basis. In this context, the EUCCS should promote an ongoing transition from narrowband critical communication systems to broadband, which is in line with the overall digital policy of the Union. Coherence with the commercial public electronic communication developments will allow critical communication to benefit also more quickly from the market-driven technological advancement of the commercial sphere.
- (13) Whereas Member States may have different models for their national critical communication systems, a set of key minimum requirements and the ability of different types of law enforcement authorities to effectively communicate between each other within a given Member State is a prerequisite for interconnecting to the European Union Critical Communication System.
- (14) Until today, critical communication was delivered usually through dedicated, self-contained networks designed to ensure availability, control, and resilience under adverse conditions. This model provided law enforcement authorities with a high degree of assurance over mission-critical communications.
- (15) Modern critical communication is however dependent on commercial, publicly available broadband networks, cloud-based services, and complex, software-defined infrastructures, meaning they are embedded within a wider and highly interdependent digital and electronic communications ecosystem. Critical communication can no longer be considered in isolation but should be approached in coherence with the security and resilience of the commercial public electronic communications networks.
- (16) It is necessary to lay down a set of minimum requirements for the resilience and security of Member States critical communication systems via this Regulation, without prejudice to Member States full sovereignty over those systems.
- (17) Critical communication systems may include or define as products with digital elements. For products with digital elements placed on the internal market, including both hardware and software, Regulation (EU) 2024/2847 of the European Parliament and of the Council²⁶ sets out cybersecurity requirements that require manufacturers to

²⁶ Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (OJ L, 2024/2847, 20.11.2024, ELI: <http://data.europa.eu/eli/reg/2024/2847/oj>, ELI: <http://data.europa.eu/eli/reg/2024/2847/oj>).

ensure a security by design approach and manage vulnerabilities during the lifecycle of the product. To facilitate the implementation for manufacturers, the requirements of the Cyber Resilience Act are being further specified by harmonised standards requested by the European Commission to the European Standardisation Organisations in line with Commission Implementing Decision C (2025)618²⁷.

- (18) The Union and its Member States should be able to operate the System without foreign interference, ensuring the confidentiality, integrity and availability of the System and of data transmitted via the System, including prohibiting the use of equipment from high-risk suppliers, especially those subject to intrusive third-country laws regarding national intelligence and data security. In this regard, the Union and its Member States should also take into account the EU ICT Supply Chain Security Toolbox²⁸ and make use of the possibility to exclude an economic operator from participation in a procurement procedure where the operator has been identified as a high-risk supplier pursuant to Regulation (EU) XXXX/XXX [CSA2 proposal]²⁹ in relation to the provision of key components for the creation, functioning or operation of the EUCCS.
- (19) Strengthening European control over key technologies required for the System is essential for its security and resilience and is also one of the priorities of the Joint Communication on strengthening Union economic security. The EUCCS should leverage the required state-of-the-art technologies and innovative solutions, thereby promoting strategic autonomy and competitiveness of the Union. The System should therefore support the continuous innovation, testing, validation and integration of emerging technologies, such as generative artificial intelligence, cloud computing, post-quantum encryption and device-to-device communication, thus ensuring it remains resilient in an evolving threat landscape.
- (20) The EUCCS can rely on the use of dedicated spectrum to ensure interoperability and continuous availability. Commission Implementing Decision (EU) 2016/687³⁰ enables Member States, subject to national decisions and choice, to designate and make available up to 8 MHz of paired spectrum for critical communications within the 700 MHz frequency band. Member States should exchange experience and best practice through the Radio Spectrum Policy Group to facilitate the coordinated designation and

²⁷ Commission Implementing Decision C (2025)618 of 3 February 2025 on a standardisation request to the European Committee for Standardisation (CEN), the European Committee for Electrotechnical Standardisation (Cenelec) and the European Telecommunications Standards Institute (ETSI) as regards products with digital elements in support of Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products, with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act).

²⁸ EU ICT Supply Chain Toolbox, NIS Cooperation Group, https://digital-skills-jobs.europa.eu/sites/default/files/2026-02/NISCG_2026_EU_ICT_Supply_Chain_Security_Toolbox_j7C7mjtm8bJ7UHDEltXtl2CDXS0_124_123.pdf

²⁹ [...]

³⁰ Commission Implementing Decision (EU) 2016/687 of 28 April 2016 on the harmonisation of the 694-790 MHz frequency band for terrestrial systems capable of providing wireless broadband electronic communications services and for flexible national use in the Union (OJ L 118, 4.5.2016, p. 4, ELI: http://data.europa.eu/eli/dec_impl/2016/687/oj).

availability of EU-harmonised spectrum for critical communications in accordance with that Implementing Decision.

- (21) Furthermore, Article 17 of Regulation [...] of the European Parliament and of the Council [on digital networks, amending Regulation (EU) 2015/2120, Directive 2002/58/EC and Decision No 676/2002/EC and repealing Regulation (EU) 2018/1971, Directive (EU) 2018/1972 and Decision No 243/2012/EU (Digital Networks Act)]³¹ provides that the Union spectrum strategy shall identify radio spectrum needs and ensure availability and, where relevant, protect radio spectrum necessary for fulfilling objectives of different Union policy areas involving the use of radio spectrum, including critical communications.
- (22) Regulation (EU) XXXX/XXX [The Digital Networks Act] recognises the role of critical communication, that enable emergency services and public authorities in charge of security and safety to fulfil their mission and should therefore be fully available on public communication networks. Consequently, providers of electronic communications networks and services should adopt specific measures to ensure uninterrupted electronic communications, including internet traffic, to the extent necessary to effectively conduct emergency response.
- (23) Critical communications may be supported by new technologies, like network slicing, which should benefit from sufficient network capacity to ensure quality of service in crisis situations. If necessary to ensure the quality of such services, the related traffic should be prioritised and redundancy for continued availability of critical communications should be ensured.
- (24) Critical communication can be provided in the exercise of public powers³² for the fulfilment of sovereign missions related to public security, safety and emergency response, and therefore may fall outside the scope of internal market and competition rules. Member States maintain competency to regulate the operational and financial conditions of these services at the national level, in line with the applicable Union law. Where the same communications infrastructure is used for the provision of both commercial and critical communications services, appropriate safeguards may prevent possible cross-subsidisation or overcompensation.
- (25) In order to ensure the technical feasibility of seamless and continuous access to the European Union Critical Communication System, it is necessary to establish common technical and interoperability requirements enabling the mission critical interconnection, interoperability and continuity of communications between Member States' critical communication systems. Standards are therefore required to ensure operational mobility for law enforcement authorities across the Union and the Schengen area, to guarantee interoperability between national mission-critical communication systems. Compliance with such harmonised standards should provide

³¹ COM(2026) 16 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52026PC0016>
³² [Services of general interest - European Commission](#)

one of the means to demonstrate conformity with the requirements laid down in this Regulation.

- (26) In order for the European Union Critical Communication System to function, it is essential that Member States' systems are compliant with a set of minimum requirements, including readiness to interconnect with the systems of other Member States. In order to accredit Member States' systems readiness for inclusion into the System in line with the security assurance levels laid out in the Regulation (EU) XXXX/XXX of the European Parliament and the Council [on establishing a framework of measures for strengthening Europe's cloud and AI ecosystem]³³, it is necessary to establish a System Accreditation Board. Its activities should cover the verification of Member States' critical communication systems interconnection, roaming readiness, rollout of baseline mission critical services and key enabling capabilities, as well as alignment with the European Union Critical Communication System security and resilience. The Board will ensure that Member States retain the key role in accrediting critical communication systems, while at the same time ensuring the necessary level of trust that is needed to perform their interconnection. The assessment of the Board will be formalised by the Commission which adopts the decision on the accreditation.
- (27) Member States have different starting points and the transition into mission critical broadband will happen in different timelines. Therefore, a gradual approach in which Member States connect in three groups from 2030 onwards, with 2036 as the final date for transition and interconnection.
- (28) A European Union Network Monitoring Centre should be set up by the Commission by outsourcing its cybersecurity and network management tasks. The centre should operate as virtual entity to provide a specific service, thus removing the need to create any official body. It should support the interconnection of Member States' critical communication systems and monitor the availability, performance, and continuity of service. To facilitate the interconnection of Member States' critical communication systems, it is appropriate for the Union to provide a central mission critical interconnection infrastructure. A central interconnection node should be established to connect Member States' systems, thus removing the need for a high number of bilateral or regional interconnections.
- (29) In order to ensure operational integrity, detect, assess and mitigate security threats to the European Union Critical Communication System, it is necessary to establish a European Union Security Monitoring Centre, using the same approach as for the Network Monitoring Centre. It should cooperate closely with the Network Monitoring Centre through continuous information exchange and coordinated incident-management procedures. As per established practice in the telecommunication and cyber security domain, the Security Monitoring Centre is separated from the Network Monitoring Centre.

³³ COM(2026) 502 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52026PC0502>

- (30) The Commission should facilitate cooperation among Member States and the exchange of information, including best practices, on issues relating to this Regulation with the support of a European Union Critical Communication Group, consisting of experts from Member States.
- (31) To ensure the resilience and continuity of critical communications for emergency services, it is necessary to integrate non-terrestrial networks, including secure satellite connectivity, as a backup and supplementary capability where terrestrial networks are unavailable, degraded, overloaded, or compromised. The Union Secure Connectivity Programme (IRIS²), established by Regulation (EU) 2023/588 of the European Parliament and of the Council³⁴, and the Governmental Satellite Communication (GOVSATCOM) component, established by Regulation (EU) 2021/696 of the European Parliament and of the Council³⁵, provide the secure and scalable infrastructure required to complement terrestrial networks in such scenarios. Access to these systems remains subject to the decision-making authority of the GOVSATCOM and IRIS² Competent Authorities and should respect the primary mission or operational priorities of IRIS² or GOVSATCOM.
- (32) Use of satellite connectivity within the EUCCS should be operationally driven, based on authorisation by the competent authorities, technically feasible, and authorised, with clearly defined service modes—including stationary backup, communication-on-the-pause, communication-on-the-move, and direct-to-device connectivity to address the diverse needs of law enforcement authorities. Such use should be granted only where capacity and budgetary resources are available, and should be governed by interoperability, security, and prioritisation rules to ensure alignment with Union law and the operational requirements of Member States.
- (33) When providing mobile satellite services (MSS) using the harmonised 2 GHz frequency band, it is essential that sufficient MSS spectrum and capacity for broadband and Direct-to-Device connectivity will be available for the EUCCS.
- (34) The EUCCS is built on more than 10 years of Union funded research and deployment projects. It is essential to continue to provide Member States, law enforcement authorities and industry a framework for technical cooperation, innovation and testing, building on the results of the projects Horizon 2020 Broadmap, Broadway and EUCCS Preparation Project. Their results are fundamental for the development of Member State pilot projects, for the organisation of large-scale exercises and trials of the System and the Member States' interconnections, to promote sharing of feedback for evolving operational requirements and as a testbed for testing and validating updated or new technological solutions before deployment.

³⁴ Regulation (EU) 2023/588 of the European Parliament and of the Council of 15 March 2023 establishing the Union Secure Connectivity Programme for the period 2023-2027 (OJ L 79, 17.3.2023, p. 1, ELI: <http://data.europa.eu/eli/reg/2023/588/oj>).

³⁵ Regulation (EU) 2021/696 of the European Parliament and of the Council of 28 April 2021 establishing the Union Space Programme and the European Union Agency for the Space Programme and repealing Regulations (EU) No 912/2010, (EU) No 1285/2013 and (EU) No 377/2014 and Decision No 541/2014/EU (OJ L 170, 12.5.2021, p. 69, ELI: <http://data.europa.eu/eli/reg/2021/696/oj>).

- (35) The System should furthermore provide the basis for the roll-out and use of increasingly harmonised solutions for communication and situational awareness at a Union level, including notably solutions piloted by Union funded initiatives. This is in line with the EUCCS architecture, which follows a system of systems approach, in which Member States' critical communication systems interact and collaborate on the basis of common standards and rules, resulting in enhanced functionalities and performance beyond the capabilities of the individual systems.
- (36) This Regulation respects fundamental rights and observes the principles recognised by Articles 2 and 6 of the Treaty on European Union and reflected in the Charter of Fundamental Rights of the European Union.
- (37) Where, under this Regulation, personal data are processed, such processing should be carried out in accordance with applicable Union and national law on the protection of personal data. Given that critical communication systems are operated at national level and remain under the responsibility of the Member States, the processing of personal data carried out through such systems should continue to be subject to the applicable data protection regime governing the respective national or Union actors involved. Any processing of personal data under this Regulation is therefore subject, as applicable, to Regulation (EU) 2016/679 of the European Parliament and of the Council³⁶, Directive (EU) 2016/680 of the European Parliament and of the Council³⁷, and Regulation (EU) 2018/1725 of the European Parliament and of the Council³⁸.
- (38) The EUCCS represents a trans-European digital public service within the meaning of Regulation (EU) 2024/903 of the European Parliament and of the Council³⁹. An interoperability assessment has thus been carried out, and the resulting report will be published on the Interoperable Europe Portal.
- (39) In order to ensure the interconnection, at Union level, of the Member States critical communication systems used by competent law enforcement authorities, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission in respect of establishing the

³⁶ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1, ELI: <http://data.europa.eu/eli/reg/2016/679/oj>).

³⁷ Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89, ELI: <http://data.europa.eu/eli/dir/2016/680/oj>).

³⁸ Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39, ELI: <http://data.europa.eu/eli/reg/2018/1725/oj>).

³⁹ Regulation (EU) 2024/903 of the European Parliament and of the Council of 13 March 2024 laying down measures for a high level of public sector interoperability across the Union (Interoperable Europe Act) (OJ L, 2024/903, 22.3.2024, ELI: <http://data.europa.eu/eli/reg/2024/903/oj>).

list of relevant standards related to critical communication. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making⁴⁰. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.

- (40) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission on establishing minimum requirements for the security and resilience of the Member States' critical communication systems, on laying down procedural arrangements necessary for the functioning and decision-making of the System Accreditation Board, on the decision on granting or refusing the accreditation to the Member States' critical communication system, on laying down standard operating procedures for the Member States' competent law enforcement authorities for the use of the system for interagency and cross-border critical communications, on required capacity, capabilities, technical standards, governance, security, and accreditation for the use of satellite connectivity within the system, on the prioritisation and service allocation procedures between users at national level, ensuring uninterrupted access for law enforcement authorities.
- (41) Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council⁴¹.
- (42) The objectives of this Regulation of enhanced cooperation among law enforcement authorities across borders cannot be sufficiently achieved by the Member States individually but can rather by reason of enhanced cooperation among law enforcement authorities across borders be better achieved at Union level. The Union may therefore adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality, as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve those objectives.
- (43) In accordance with Articles 1 and 2 of Protocol No 22 on the position of Denmark annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, Denmark is not taking part in the adoption of this Regulation and is not bound by it or subject to its application. Given that this Regulation builds on the Schengen acquis, to the extent that it applies to cross-border cooperation between law enforcement authorities, Denmark shall, in accordance with Article 4 of that Protocol,

⁴⁰ OJ L 123, 12.5.2016, p. 1, ELI: http://data.europa.eu/eli/agree_interinstit/2016/512/oj.

⁴¹ Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13, ELI: <http://data.europa.eu/eli/reg/2011/182/oj>).

decide within a period of six months after the Council has decided on this Regulation whether it will implement it in its national law.

- (44) As regards Ireland, this Regulation constitutes a development of the provisions of the Schengen *acquis* in which Ireland takes part, in accordance with Council Decision 2002/192/EC of 28 February 2002 concerning Ireland's request to take part in some of the provisions of the Schengen *acquis*. Ireland is therefore bound by this Regulation and subject to its application.
- (45) As regards Iceland and Norway, this Regulation constitutes a development of the provisions of the Schengen *acquis* within the meaning of the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the latter's association with the implementation, application and development of the Schengen *acquis*⁴², which fall within the area referred to in Article 1, point G, of Council Decision 1999/437/EC.
- (46) As regards Switzerland, this Regulation constitutes a development of the provisions of the Schengen *acquis* within the meaning of the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis*⁴³, which fall within the area referred to in Article 1, point G, of Decision 1999/437/EC, read in conjunction with Article 3 of Council Decision 2008/146/EC⁴⁴.
- (47) As regards Liechtenstein, this Regulation constitutes a development of the provisions of the Schengen *acquis* within the meaning of the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis*⁴⁵ which fall within the area referred to in Article 1, point G, of Decision 1999 /437/EC read in conjunction with Article 3 of Council Decision 2011/350/EU⁴⁶,

⁴² OJ L 176, 10.7.1999, p. 36, ELI: [http://data.europa.eu/eli/agree_internation/1999/439\(1\)/oj](http://data.europa.eu/eli/agree_internation/1999/439(1)/oj).

⁴³ OJ L 53, 27.2.2008, p. 52, ELI: [http://data.europa.eu/eli/agree_internation/2008/178\(1\)/oj](http://data.europa.eu/eli/agree_internation/2008/178(1)/oj).

⁴⁴ Council Decision 2008/146/EC of 28 January 2008 on the conclusion, on behalf of the European Community, of the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis* (OJ L 53, 27.2.2008, p. 1, ELI: <http://data.europa.eu/eli/dec/2008/146/oj>).

⁴⁵ OJ L 160, 18.6.2011, p. 21, ELI: <http://data.europa.eu/eli/prot/2011/349/oj>.

⁴⁶ Council Decision 2011/350/EU of 7 March 2011 on the conclusion, on behalf of the European Union, of the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis*, relating to the abolition of checks at internal borders and movement of persons (OJ L 160, 18.6.2011, p. 19, ELI: <http://data.europa.eu/eli/dec/2011/350/oj>).

- (48) The European Data Protection Supervisor was consulted in accordance with Article 42 of Regulation (EU) 2018/1725 of the European Parliament and of the Council and delivered an opinion on [„„].

HAVE ADOPTED THIS REGULATION:

CHAPTER I

GENERAL PROVISIONS

Article 1

Subject matter

This Regulation establishes the European Union Critical Communication System (EUCCS) which interconnects, at Union level, the Member States' critical communication systems used by competent law enforcement authorities to ensure secure and reliable connectivity for those systems.

Article 2

Responsibilities and duties of the Member States

1. Member States shall ensure that their national critical communication systems used by competent law enforcement authorities are interoperable so that they can be interconnected at Union level.
2. This Regulation shall apply to critical communication systems used by any authority of the Member States competent under national law to exercise authority and to take coercive measures for the purpose of preventing, detecting or investigating criminal offences, including those carrying out the following functions:
 - (a) policing;
 - (b) border control as defined in Article 2, point 10 of Regulation (EU) 2016/399 of the European Parliament and of the Council ⁴⁷;
 - (c) coast guard functions;
 - (d) customs controls as defined in Article 5, point (27) of Regulation (EU) 2026/2108⁴⁸.
3. Member States shall ensure that the European Union Agency for Law Enforcement Cooperation (Europol) is granted access to use the EUCCS in line with its mandate.
4. Member States shall ensure that the European Border and Coast Guard Agency (Frontex) is granted access to use the EUCCS, including the European Operational Support in accordance with Chapter VI, for all operational activities in line with its mandate.

⁴⁷ Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code) (OJ L 77, 23.3.2016, p. 1, ELI: <http://data.europa.eu/eli/reg/2016/399/oj>).

⁴⁸ Regulation (EU) 2026/2108 of the European Parliament and of the Council of 16 September 2026 establishing the Union Customs Code and the European Union Customs Authority, and repealing Regulation (EU) No 952/2013 (OJ L, 2026/2108, 19.9.2026, ELI: <http://data.europa.eu/eli/reg/2026/2108/oj>).

5. Member States shall ensure that the European Union Customs Authority is granted access to use the EUCCS in line with its mandate.

Article 3

Definitions

1. For the purpose of this Regulation, the following definitions apply:
 - (1) ‘competent law enforcement authorities’ means any police, customs or other authority of the Member States competent under national law to exercise authority and to take coercive measures for the purpose of preventing, detecting or investigating criminal offences including to maintain security and public order;
 - (2) ‘critical communication’ means electronic communication that is not publicly available, and which is essential for communication in emergencies and crisis situations and for restoring or maintaining security and public safety;
 - (3) ‘users of critical communications’ means physical or legal persons that provide public services of critical nature whose effective provision of which may require situational awareness or confidential and uninterrupted communication and that are recognised by Member States as such;
 - (4) ‘critical communication services’ means standardised electronic communication services that provide enabling capabilities for competent law enforcement authorities and other public authorities in charge of security and safety;
 - (5) ‘non-terrestrial network’ means a network, or segments of a network, that use an airborne or space-borne platform to host transmission equipment, which can function as a relay node or a base station;
 - (6) ‘critical communication interconnection’ means the resilient technical and operational linking of national critical communication systems via a network of dedicated connectivity means, -such as fibre optics-, therefore enabling cross-border critical communication;
 - (7) ‘public network’ means a public electronic communications network that is not dedicated to governmental or mission-critical use;
 - (8) ‘radio access network’ means the part of a mobile network that connects user devices to the mobile core network;
 - (9) ‘critical communication core’ means a mobile core network in accordance with applicable European Telecommunications Standards- used for critical communication that serves users separately from publicly available electronic communication services and includes additional safeguards in terms of resilience, and security to ensure guaranteed service and reliability providing users with optimal quality of service, priority and pre-emption over commercial users in emergency situations where Radio Access resources are shared;

- (10) ‘broadband critical communication’ means IP based packet switched critical communication that enables Gigabit connectivity and real-time data, video, text, voice and conferencing services;
- (11) ‘narrowband critical communication’ means critical communication that is not based on mission critical broadband, such as those defined under ETSI EN 300 392-1;
- (12) ‘harmonised standard’ means a harmonised standard as defined in Article 2(1), point (c), of Regulation (EU) No 1025/2012⁴⁹.

CHAPTER II

FRAMEWORK FOR CRITICAL COMMUNICATION IN THE MEMBER STATES

Article 4

Competent authorities

1. Each Member State shall designate a competent authority which shall have at least the following tasks:
 - (a) prepare and implement the critical communication strategy as referred to in Article 5;
 - (b) ensure the overall functioning, resilience and security of the critical communication system in that Member State, including ensuring that it is used in compliance with the interoperability, security, resilience and operational requirements laid down by this Regulation;
 - (c) oversee the evolution of the critical communication system of that Member State from narrowband towards broadband critical communication, as well as any other technological development affecting critical communication;
 - (d) supervise personnel, networks and equipment necessary for the functioning of the critical communication system of the Member State and take the measures to allow for its interconnection with other Member States’ systems;
 - (e) ensure that providers of public electronic communications networks comply with obligations in relation to Article 8 of this Regulation;
 - (f) act as single point of contact for the Commission and for the other competent authorities for the purpose of the implementation of this Regulation;

⁴⁹ Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council (OJ L 316, 14.11.2012, p. 12, ELI: <http://data.europa.eu/eli/reg/2012/1025/oj>).

- (g) nominate a representative to the System Accreditation Board referred to in Article 10;
 - (h) carry out pilot projects for the further development of the EUCCS, using dedicated parts of the critical communication system of the Member State as testbeds, validating and integrating state-of-the-art technologies and innovative solutions before deployment of those deployments.
2. By 3 months after the entry into force of this Regulation at the latest each Member State shall notify its competent authority to the Commission.
 3. Each Member State shall ensure that its competent authority has the powers and the adequate financial, human and technical resources to carry out, in an effective and efficient manner, the tasks assigned to it.
 4. Each Member State shall ensure that its competent authority, whenever appropriate, and in accordance with Union and national law, consults and cooperates with other relevant authorities, including the national competent authority established in accordance with Article 68(4) of Regulation (EU) 2021/696 and Article 11(4) of Regulation (EU) 2023/588.

Article 5

Critical Communication Strategy of the Member State

1. Member State shall adopt and transmit to the Commission a critical communication strategy. That strategy shall set out the measures required for the transition from existing narrowband to broadband and packet switched critical communication, as well as for the interconnection of the critical communication system of the Member State to the systems of other Member States.
2. The critical communication strategy shall include at least the following elements:
 - (a) defining the users of the Member State's critical communication system;
 - (b) determining the framework for procurement for the purposes of the transition to the broadband critical communication system and of the interconnection via the critical communication interconnection infrastructure established on the basis of commercial agreements with providers of publicly available electronic communication networks;
 - (c) setting out the framework for the strategic collaboration with providers of publicly available electronic communication networks and their role to ensure the resilience of critical communication services;
 - (d) describing the deployment of the Member State's critical communication system in line with Article 6 and the measures to ensure its resilience in line with Article 7;
 - (e) ensuring its coherence with national broadband plans;
 - (f) determining the transition period for narrowband critical communication systems;
 - (g) outlining investment plans and envisaged funding;

- (h) setting out the steps to be taken for interconnection with other Member States' critical communication systems;
 - (i) setting out a framework and schedule for regular monitoring and, where appropriate, adaptation of the national critical communication system to the continuous innovation in critical communication and commercial electronic communications, ensuring the future-proof evolution of its critical communication system.
- 3. Member States shall regularly review and, where appropriate, update their critical communication strategies and communicate any updates to the Commission upon their adoption.

Article 6

Critical communication system of Member States

1. Critical communication system of a Member State shall consist as a minimum of the following components:
 - (a) radio access network;
 - (b) critical communication core;
 - (c) critical communication services.
2. In accordance with the deadlines and requirements laid down in this Regulation and the maturity levels set out in the Annex, each Member State shall establish its-critical broadband communication system using existing network infrastructures offered by providers of publicly available electronic communication networks to the extent possible and appropriate on a shared basis using advanced traffic differentiation techniques such as network slicing. Member States may use narrowband systems for their critical communication systems as back-up and for providing additional coverage.
3. Each Member State shall ensure that its critical communication system is able to establish an interconnection with the critical communication systems of other Member States by complying with the standards as defined under Article 11.
4. Member States shall exchange best practices on the use of EU-harmonised spectrum suitable for critical communications in accordance with Implementing Decision (EU) 2016/687.
5. Member States shall ensure that services, systems and interconnection components used for their critical communication system comply with standards as referred to in Article 11 and are subject to conformity assessment, certification, interoperability testing and field validation.
6. Member States may carry out pilot projects for the further development of the System, including via the use of dedicated parts of the Member States' critical communication systems as for testing, validating and integrating state-of-the-art technologies and innovative solutions before deployment.

Resilience of Member States' critical communication systems

1. Member States shall ensure a high level of resilience and security of their critical communication systems. For that purpose, Member States shall:
 - (a) take appropriate and proportionate technical, operational and organisational measures that reflect the principles of security by design and by default to ensure the cybersecurity of the critical communication systems and its components, including, where relevant, measures listed in Article 21(2) of Directive (EU) 2022/2555 of the European Parliament and of the Council⁵⁰;
 - (b) take appropriate and proportionate technical, security and organisational measures to ensure the resilience of the critical communication systems and its components, including, where relevant, measures listed in Article 13(1) of Directive (EU) 2022/2557⁵¹;
 - (c) meet pre-defined specific requirements to ensure the highest level of resilience and appropriate separation end-to-end from any publicly available commercial communications services. Such separation may be achieved through physical, logical, technical, operational, organisational and/or contractual measures, provided that those measures effectively guarantee the required level of security, resilience, availability and control. Such separation shall not preclude the deployment of critical communication services over public electronic communications networks on a shared infrastructure basis;
 - (d) ensure the sovereignty, the exclusion of high-risk suppliers and overall supply chain security related to the Critical Communication Core and any other key ICT assets, in accordance with Regulation (EU) XXX/XXXX of the European Parliament and the Council [on the European Union Agency for Cybersecurity (ENISA), the European cybersecurity certification framework, and ICT supply chain security and repealing Regulation (EU) 2019/881]⁵²;
 - (e) ensure that critical communication data is not subject to third country legislation requiring providers to grant, assist or support access to their authorities or any other party.
2. Member States shall establish their critical communication security operations centre. Those centres shall ensure the secure operation of the national critical communications system and cooperation with the European Union Security Monitoring Centre referred to in Article 15. Member States shall notify those centres to the Commission upon establishment.
3. The Commission is empowered to adopt an implementing act establishing minimum requirements for the security and resilience of the Member States' critical

⁵⁰ Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 333, 27.12.2022, p. 80, ELI: <http://data.europa.eu/eli/dir/2022/2555/oj>)

⁵¹ Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (OJ L 333, 27.12.2022, p. 164, ELI: <http://data.europa.eu/eli/dir/2022/2557/oj>)

⁵² [COM(2026) 11 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52026PC0011>]

communication systems. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 22(2).

4. This Regulation shall not preclude Member States from adopting or maintaining provisions of national law with a view to achieving a higher level of resilience of critical communication systems, provided that such provisions do not interfere with Member States' obligations laid down in Union law.

Article 8

Use of public electronic communications networks for critical communication

1. Member States shall ensure the availability of public electronic communications networks to convey critical communications with the level of quality required to ensure its uninterrupted availability and effective functioning, including in emergency and crisis situations subject to the relevant commercial agreements with providers of such public electronic communication services. Such level of quality shall take into account relevant technical parameters, including latency, jitter, packet loss and throughput.
2. In situations of network congestion, or other duly justified cases, Member States shall ensure that providers of public electronic communications networks implement traffic management measures ensuring prioritisation and pre-emption of traffic related to critical communication, in accordance with Article 3 of Regulation (EU) 2015/2120 of the European Parliament and of the Council⁵³.
3. Remuneration for the conveyance of critical communications over public electronic communications networks, including data, shall be subject to commercial agreements between the relevant parties and shall be based on fair and reasonable terms and conditions. Such remuneration shall not be excessive.

CHAPTER III

UNION-LEVEL GOVERNANCE

Article 9

European Union Critical Communication Group

1. The European Union Critical Communication Group ('the Group') is established.
2. The Group shall be composed of one representative for each of the Member States, which are nominated by Competent Authorities and notified to the Commission, and one representative of the Commission, nominated by the Director-General of the

⁵³ Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union (OJ L 310, 26.11.2015, p. 1, ELI: <http://data.europa.eu/eli/reg/2015/2120/oj>).

Directorate for Internal Affairs and Migration of the European Commission. The Commission's representative shall chair the Group. Where relevant for the performance of its tasks, the Group may nominate permanent observers or invite relevant stakeholders and other Commission services to participate in its work, including the meetings of the Group. Where requested by the European Parliament, the Chair may invite a representative from the European Parliament to attend one or several meetings of the Group.

3. The Group's tasks include:

- (a) providing strategic guidance to Member States on the establishment and further development of the System and the Member States' components;
- (b) collecting, exchanging and making available to relevant stakeholders best practices on matters related to critical communication, such as resilience, security, operational aspects, procurement or innovation;
- (c) contributing to the preparation of implementing and delegated acts stemming from this Regulation;
- (d) reviewing and, where appropriate, providing input on the Mission Critical Broadband Strategies as referred to in Article 5;
- (e) providing guidance for Member States on compliance with Article 7(1), points (c) and (d);
- (f) cooperating with relevant Union institutions, bodies and agencies, third countries or international organisations on matters related to this Regulation;
- (g) monitor the progress of standardisation related to critical communication and cooperate with relevant standardisation organisations;
- (h) adopting non-binding guidance or recommendations on matters related to critical communication;
- (i) reviewing the outcome of assessment missions as referred to in Article 13 and, where appropriate, making use of the results of such missions in the identification of best practices according to point (b) of this paragraph and in the provision of guidance and recommendations according to point (h) of this paragraph;
- (j) where relevant, assisting the Commission in the development of related policies and documents, including on internal security, digital transition, space connectivity or civil protection;
- (k) exchanging on any topic relevant for critical communication.

Article 10

System Accreditation Board

- 1. A System Accreditation Board ('the Board') is established.
- 2. The Board shall be composed of a representative of each Member State, nominated by the competent authority, and of a representative of the Commission. Representatives of Member States shall be duly qualified in the field of critical communication and accrediting communication systems, have an appropriate level of security clearance, where necessary, and act objectively.

3. The Board shall assess Member States' systems readiness for connection to the EUCCS, on the basis of maturity levels set out in the Annex. The Board shall assess the readiness of the Member State system, based on assessment missions in accordance with Article 13 and on any other relevant information after notification by the Member State of the readiness of the national system for accreditation.
4. The Board shall send to the Commission the outcome of the assessment without undue delay and where possible within three months of the notification.
5. The Commission may adopt implementing acts laying down procedural arrangements necessary for the functioning and decision-making of the Board. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 22(2).

CHAPTER IV

SYSTEM ACCREDITATION AND INTERCONNECTION

Article 11

Standards and general principles of accreditation and interconnection

1. Member States' critical communication systems shall, in order to be accredited, comply with European and international standards and technical specifications related to critical communication covering at least the following requirements:
 - (a) the proper functioning and interoperability of the components laid down in Article 6(1);
 - (b) the use of broadband critical communication systems that use existing public electronic communication network infrastructures laid down in Article 6(2);
 - (c) the ability of a Member States' critical communication system to establish an interconnection with the critical communication systems of other Member States laid down in Article 6(3);
 - (d) technical, security and organisational measures to ensure the resilience and cybersecurity of critical communication systems as laid down in Article 7(1);
2. The Commission shall adopt a delegated act to supplement the requirements for critical communication systems of Member States referred to in paragraph 1 by establishing the list of relevant standards.
3. Member States shall ensure compliance of their critical communication systems with the standards referred to in this Article and shall pursue accreditation of those systems by requesting the Board to accredit the national system and ensuring full cooperation of all relevant entities during the accreditation process.
4. Taking into account the outcome of the assessment of the critical communication system by the Board, referred to in Article 10(3), the Commission shall decide on granting or refusing the accreditation, by means of an implementing act. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 22(2).

5. When their critical communication system is accredited, Member States shall ensure the interconnection of their national system via the critical communication interconnection infrastructure referred to in Article 13 and in accordance with Article 14.

Article 12

Assessment missions

1. Upon receipt of a request for accreditation of a critical communication system of a Member States, the Commission shall organise a mission to assess the compliance with the requirements for accreditation set out in this Regulation and with the standards referred to in Article 11.
2. In duly justified cases, the Board may also request the Commission to organise a mission to a Member State whose critical communication system has already been accredited to verify continuous compliance.
3. The Commission may request Member States to provide information before a mission, notably on the functioning of the Member States' critical communication framework, national legal provisions affecting the components of the Member States' critical communication system, standards adhered to, certifications obtained, as well as system and interconnection technical performances, compliance with requirements relating to the relevant the maturity levels of the EUCCS set out in the Annex.
4. The Commission shall, following a consultation with the Member State whose critical communication system is assessed, select and appoint the members of each mission. Each mission shall consist of experts from the Member State, experts from any other Member States and Commission representatives. Additional experts, including from Union Agencies or bodies, may be nominated as observers by the Commission to join a mission.
5. Member States shall ensure that entities involved in their national critical communication system provide missions with full and unhindered access to information, systems and facilities, without prejudice to that Member State's responsibility for national security and the protection of its security interests.
6. The Commission, based on the findings of the mission, shall communicates its opinion to the Board and the Member State whose critical communication system was assessed.
7. The Member State that hosts the critical communication system shall ensure that its competent authority and entities involved in the critical communication system concerned take into account the findings and provide information to the Commission and Board on the measures it has taken pursuant to the findings of the mission.
8. The Board shall consider the findings of the mission in its decision for accreditation of a Member State's system.

Article 13

Critical communication interconnection infrastructure

1. The Commission shall make available a critical communication interconnection infrastructure that facilitates the interconnection of Member States' systems. The Critical Communication Interconnection infrastructure shall:
 - (a) provide connectivity dedicated to communications and information exchange between Member States' critical communication systems;
 - (b) ensure confidentiality, integrity and availability of communications and related data;
 - (c) be designed to remain operational and performant, including during crises affecting all electronic communication networks used for critical communications.
2. The Critical Communication interconnection infrastructure shall use an existing Union secure network for communications to connect Member States' critical communication systems.
3. The critical communication interconnection infrastructure shall be designed and operated to minimise exposure to threats and reduce any attack surface.
4. The Commission and the Member States shall ensure continuity of service for the interconnection by taking resilience measures that are coherent with the measures taken under Article 7.

Article 14

Gradual establishment

1. Interconnection of the accredited critical communication systems of the Member States shall be implemented in three stages:
 - (a) the first stage shall start on 1 December 2030, as provided for in paragraph 2;
 - (b) the second stage shall start on 1 December 2033, as provided in paragraph 3;
 - (c) the third stage shall start on 1 December 2036, as provided in paragraph 4.
2. Member States whose critical communication systems comply with the requirements for the initial maturity level as set out in the Annex and have been accredited by the Commission under the conditions set out in Article 11(4) by the dates referred to in paragraph 1, point (a) shall interconnect their systems with other Member States' accredited systems in the first stage.
3. Member States whose critical communication systems comply with the requirements for the initial and advanced maturity levels as set out in the Annex and have been accredited by the Commission under the conditions set out in Article 11(4) by the date referred to in paragraph 1, point (b) shall interconnect their systems with other

Member States' accredited systems in the second stage. The Member States referred to in paragraph 2 shall comply with the requirements for the advanced maturity level by the date referred to in paragraph 1, point (b).

4. All Member States shall ensure that their critical communication systems comply with the requirements for the initial, advanced and optimal maturity levels as set out in the Annex and that those systems have been accredited by the Commission pursuant to Article 11(4) under the conditions set out in Article 10 by the date referred to in paragraph 1, point (c).
5. The Commission shall make publicly available the list of Member States that are to be included in the stages as defined in paragraph 1.
6. The EUCCS shall commence operations from the date referred to in paragraph 1, point (a).
7. Member States may engage in bilateral or regional interconnection of their critical communication systems prior to the dates referred to in paragraph 1, provided those systems comply with the requirements set out in this Regulation.
8. Member States may engage with neighbouring third countries and territories that do not contravene the interests of the Union, in view of establishing targeted interconnection between respective critical communication systems, provided the third country or territories' critical communication system abides to the standards as referred to in Article 11.
9. Before pursuing bilateral, or regional, interconnection as referred to in paragraphs 7 and 8, concerned Member States shall notify the Commission prior to the start of the interconnection, and the Commission shall in turn inform the Board and the Group without delay.

CHAPTER V

EUROPEAN UNION COMPONENTS

Article 15

European Union Critical Communication Network Monitoring Centre

1. The Commission shall establish a European Union Critical Communication Network Monitoring Centre ('Network Monitoring Centre') for the System by 1 December 2029.
2. The European Union Critical Communication Network Monitoring Centre shall perform, inter alia, the following tasks:
 - (a) host the Critical communication interconnection infrastructure;
 - (b) support the interconnection of Member States' critical communication systems as referred to in Article 14;

- (c) monitor the availability, performance, and continuity of Union-level critical communication roaming and interconnection;
 - (d) enable the roaming of users of critical communication systems across Member States;
 - (e) monitor transmission for cross-border operational needs, including critical communication roaming authentication and authorisation arrangements for visiting users of the Member States' critical communication systems;
 - (f) support cross-border testing of critical communications roaming functionality and interoperability between Member States' critical communication systems.
3. The Network Monitoring Centre shall cooperate closely with the European Security Monitoring Centre and shall provide it, without undue delay, with network events, performance information and other operational data necessary for cybersecurity monitoring, incident detection and response.
 4. The Network Monitoring Centre's activities shall be without prejudice to the provisions of Regulation (EU, Euratom) 2023/2841 of the European Parliament and of the Council⁵⁴.

Article 16

European Union Critical Communication Security Monitoring Centre

1. The Commission shall establish a European Security Monitoring Centre ('Security Monitoring Centre') to collect and aggregate information on threats to the System by 1 December 2029.
2. To this end, the Member States' Critical Communication Security Operations Centres as referred to in Article 7 shall provide reports on a regular basis concerning security incidents, vulnerabilities and risks affecting the System to the European Security Monitoring Centre. A Critical Communication Security Operations Centre shall notify any incident that interferes with or interrupts the functioning of the national critical communications system or of its interconnection ('critical incident') to the Security Monitoring Centre without delay and latest within [48 hours] of the discovery of the incident.
3. The European Security Monitoring Centre shall monitor the System's overall security indicators, including authentication and authorisation events, trust management, certificate status, access attempts, abnormal roaming patterns, misuse of interconnection interfaces and threats affecting the communication infrastructure.
4. The Security Monitoring Centre and the Network Monitoring Centre shall provide evidence to the System Accreditation Board for its decisions to accredit a Member State system, or to verify its continuous compliance, by assessing the security, cybersecurity and resilience requirements for the Member States' critical communication systems and their interconnections.

⁵⁴ Regulation (EU, Euratom) 2023/2841 of the European Parliament and of the Council of 13 December 2023 laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union (OJ L, 2023/2841, 18.12.2023, ELI: <http://data.europa.eu/eli/reg/2023/2841/oj>).

5. The Security Monitoring Centre shall support testing of security controls for roaming authentication and authorisation, trust management, interconnection interfaces and mission-critical service interoperability.
6. The Security Monitoring Centre shall issue recommendations, propose mitigation measures or suggest corrective actions concerning security incidents, vulnerabilities and risks affecting Union-level critical communication roaming, communication infrastructure, users' authentication and mission-critical service interoperability. It shall provide on a regular basis reports to the Commission, the European Union Critical Communications Group, and the System Accreditation Board. In case of a critical incident as referred to in paragraph 1, it shall provide a report without undue delay. It shall cooperate with the Member States' competent authorities and cybersecurity authorities, CSIRTs Network members and relevant Union bodies and agencies to manage incidents and to follow-up on recommendations and corrective actions.

CHAPTER VI

OPERATIONAL SUPPORT

Article 17

Standard operating procedures

1. The Commission is empowered to adopt implementing acts to lay down standard operating procedures for the Member States' competent law enforcement authorities, for the consistent, efficient and compliant use of the EUCCS for interagency and cross-border critical communications. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 22(2).
2. The standard operating procedures shall lay down the roles, tasks, coordination mechanisms and protocols needed for the operational use of the System with regards to:
 - (a) the Member State competent authority referred to in Article 4;
 - (b) the cooperation of the Member State competent authority with the competent authorities designed under Regulations (EU) 2021/696 and (EU) 2023/588;
 - (c) the cooperation of the Member State competent authority with the Union Civil Protection Mechanism and Emergency Response Coordination Centre
 - (d) the operational cooperation between Member States' competent law enforcement authorities and other organisations using the EUCCS.
3. The standard operation procedures shall cover the following elements with regards to cross-border critical communications:
 - (a) defining which service leads the communication arrangements based on the incident type or location;
 - (b) establishing shared situational awareness and ensuring an efficient response;
 - (c) determining the responsibilities of the host and visiting countries' authorities at strategic, operational and tactical level;

- (d) establishing communication and interaction protocols, including for alerting, group communication, fleet-mapping and dispatching, training and joint learning.

Article 18

Use of Union Satellite Secure Connectivity services

1. Where authorised by a competent authority designed under the Regulations (EU) 2021/696 and (EU) 2023/588, the GOVSATCOM and IRIS² Competent Authorities, users and devices of the System shall employ secure satellite connectivity services provided under GOVSATCOM and IRIS² to extend, complement, or back up terrestrial networks for emergency services in cases of unavailability, degradation, overload, or compromise. The competent authorities designated under Regulations (EU) 2021/696 and (EU) 2023/588, shall retain sole discretion over the approval of such access and the allocation of resources between users. The allocation of GOVSATCOM and IRIS² capacities between users should be made in accordance with the rules defined under Regulations (EU) 2021/696 and (EU) 2023/588.
2. For back-up and complementary coverage, as well as for direct-to-device connectivity, users and devices of the EUCCS shall have access to secure governmental communications services provided by the operator of the secure MSS/hybrid system in accordance with Regulation (EU) XXX/XXXX of the European Parliament and the Council [on the procedure for authorisation of systems providing mobile satellite services using the harmonised 2 GHz frequency band and repealing Decision No 626/2008/EC]⁵⁵.
3. When the services are accessed pursuant to paragraph 1 or paragraph 2, they shall be used in the following four operational service modes:
 - (a) stationary mode in which fixed infrastructure providing backup connectivity for critical communications during terrestrial network outages;
 - (b) communication-on-the-pause in which rapidly deployable satellite connectivity for emergency services in scenarios where fixed infrastructure is temporarily unavailable or insufficient;
 - (c) communication-on-the-move in which continuous connectivity for vehicles, vessels, aircraft, and aerial platforms, enabling real-time command, control, and coordination during operations;
 - (d) direct-to-device in which satellite connectivity directly to handsets or other user equipment used by competent authorities, in line with the MSS Regulation or in the context of GOVSATCOM and IRIS², where such services are available.
4. The Commission is empowered to adopt implementing acts to specify:
 - (a) the required capacity, capabilities, and technical standards for each operational service mode referred to in paragraph 2;

⁵⁵ [COM(2026) 311 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52026PC0311>]

- (b) the governance, security, and accreditation rules for the use of satellite connectivity within the EUCCS, in accordance with the operational requirements of critical communication;
 - (c) the prioritisation and service allocation procedures between the EUCCS users at national level, ensuring uninterrupted access for law enforcement authorities without exceeding the approved capacity and budgetary limits.
- 5. In preparing the draft implementing acts, the Commission shall take into account the operational requirements of EUCCS users. Those implementing acts shall not affect the application of [Regulations \(EU\) 2021/696](#), [\(EU\) 2023/588](#) and Regulation (EU) XXX/XXX[on the procedure for authorisation of systems providing mobile satellite services using the harmonised 2 GHz frequency band and repealing Decision No 626/2008/EC].
- 6. The implementing acts referred to in paragraph 3 of this Article shall be adopted in accordance with the examination procedure referred to in Article 22(2).
- 7. Member State competent authorities designated under Article 4 of this Regulation shall cooperate with competent authorities designated under Regulations (EU) 2021/696 and (EU) 2023/588s, as well as the Commission in the context of Regulation (EU) XXX/XXX [on the procedure for authorisation of systems providing mobile satellite services using the harmonised 2 GHz frequency band and repealing Decision No 626/2008/EC] to ensure the availability, interoperability, and effective use of secure satellite connectivity services within national critical communication systems. Such cooperation shall include:
 - (a) the authorisation for the access to the services, at national level;
 - (b) the alignment of security and accreditation standards;
 - (c) the monitoring and reporting of service performance, incidents, and compliance with Union rules, including capacity usage and budgetary impacts.
- 8. For Member States participating in the EUCCS, but not participating in the relevant Union space programmes, access to non-terrestrial or secure connectivity services shall be subject to the applicable international agreements, association arrangements or specific operational agreements governing such access concluded with the Union or with participating Member States in accordance with Article 8(1) of Regulation (EU) 696/2021 and Article 40 of Regulation (EU) 588/2023.

Article 19

Commission support to Member States

1. The Commission shall support the coordination of Member States' technical and operational cooperation on critical communication.
2. The support referred to in paragraph 1 may include:

- (a) providing testbeds to prepare for the interconnection as referred to in Chapter IV;
- (b) funding of trials and exercises for emergency services to test the interoperability of critical communication systems, operational procedures or resilience of critical communication systems;
- (c) supporting Member States in cooperating with industry and research to ensure the continuous innovation of critical communication in the Union;
- (d) supporting technical cooperation projects with third countries, in particular candidate countries and potential candidates, with a view of achieving targeted interoperability;
- (e) the support referred to in paragraph 2 may be subject of Union funded projects.

CHAPTER VII

EVALUATION

Article 20

Evaluation

1. By [five years after the entry into force of this Regulation], and every five years thereafter, the Commission shall submit a report to the European Parliament and to the Council on the implementation of this Regulation, including detailed information on how each Member State has implemented it, and shall, where appropriate, propose amendments to this Regulation.
2. Member States shall, at the request of the Commission, provide it with the information necessary for the preparation of the report referred to in paragraph 1, no later than nine months before the expiry of the reporting deadline.
3. The reports referred to in paragraph 1 of this Article shall, where relevant, take into account the results of evaluations carried out pursuant to Council Regulation (EU) 2022/922⁵⁶, in particular as regards communication and the exchange of information.

CHAPTER VIII

DELEGATED AND IMPLEMENTING ACTS

⁵⁶ Council Regulation (EU) 2022/922 of 9 June 2022 on the establishment and operation of an evaluation and monitoring mechanism to verify the application of the Schengen acquis, and repealing Regulation (EU) No 1053/2013 (OJ L 160, 15.6.2022, p. 1, ELI: <http://data.europa.eu/eli/reg/2022/922/oj>).

Article 21

Exercise of the delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.
2. The power to adopt delegated acts referred to in Article 11 (2) shall be conferred on the Commission for an indeterminate period from the entry into force of this Regulation.
3. The delegation of power referred to in Article 11 (2) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.
4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making.
5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.
6. A delegated act adopted pursuant to Article 11 (2) shall enter into force only if no objection has been expressed either by the European Parliament or by the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.

Article 22

Committee procedure

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.
2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

CHAPTER IX

FINAL PROVISIONS

Article 23

Responsibilities for operation and maintenance

1. The costs incurred by the Member State for the operation, maintenance, development and modernisation of their critical communication system shall be borne by each Member State.
2. Each Member State shall set up and maintain at their expense the technical infrastructure necessary to implement their obligations under this Regulation at national level and shall be responsible for bearing the associated costs.

Article 24

Entry into force

This Regulation shall enter into force on the [...] day following that of its publication in the *Official Journal of the European Union*.

This Regulation shall be binding in its entirety and directly applicable in the Member States in accordance with the Treaties.

Done at Brussels,

For the European Parliament
The President

For the Council
The President

LEGISLATIVE FINANCIAL AND DIGITAL STATEMENT

ANNEX 4

Contents

1.	CONTEXT OF THE PROPOSAL.....	1
2.	LEGAL BASIS, SUBSIDIARITY AND PROPORTIONALITY.....	4
3.	RESULTS OF EX-POST EVALUATIONS, STAKEHOLDER CONSULTATIONS AND IMPACT ASSESSMENTS	6
4.	BUDGETARY IMPLICATIONS	11
5.	OTHER ELEMENTS	12
1.	FRAMEWORK OF THE PROPOSAL/INITIATIVE	3
1.1.	Title of the proposal/initiative	3
1.2.	Policy area(s) concerned	3
1.3.	Objective(s)	3
1.3.1.	General objective(s)	3
1.3.2.	Specific objective(s).....	3
1.3.3.	Expected result(s) and impact	5
1.3.4.	Indicators of performance	5
1.4.	The proposal/initiative relates to:.....	6
1.5.	Grounds for the proposal/initiative	6
1.5.1.	Requirement(s) to be met in the short or long term including a detailed timeline for roll-out of the implementation of the initiative	6
1.5.2.	Added value of EU involvement (it may result from different factors, e.g. coordination gains, legal certainty, greater effectiveness or complementarities). For the purposes of this section 'added value of EU involvement' is the value resulting from EU action, that is additional to the value that would have been otherwise created by Member States alone.	7
1.5.3.	Lessons learned from similar experiences in the past.....	8
1.5.4.	Compatibility with the multiannual financial framework and possible synergies with other appropriate instruments.....	8
1.5.5.	Assessment of the different available financing options, including scope for redeployment.....	9
1.6.	Duration of the proposal/initiative and of its financial impact	10
1.7.	Method(s) of budget implementation planned	10
2.	MANAGEMENT MEASURES.....	12
2.1.	Monitoring and reporting rules	12
2.2.	Management and control system(s)	12

2.2.1.	Justification of the budget implementation method(s), the funding implementation mechanism(s), the payment modalities and the control strategy proposed.....	12
2.2.2.	Information concerning the risks identified and the internal control system(s) set up to mitigate them.....	13
2.2.3.	Estimation and justification of the cost-effectiveness of the controls (ratio between the control costs and the value of the related funds managed), and assessment of the expected levels of risk of error (at payment & at closure).....	13
2.3.	Measures to prevent fraud and irregularities.....	13
3.	ESTIMATED FINANCIAL IMPACT OF THE PROPOSAL/INITIATIVE.....	14
3.1.	Heading(s) of the multiannual financial framework and expenditure budget line(s) affected.....	14
3.2.	Estimated financial impact of the proposal on appropriations.....	15
3.2.1.	Summary of estimated impact on operational appropriations.....	15
3.2.1.1.	Appropriations from voted budget.....	15
3.2.3.	Summary of estimated impact on administrative appropriations.....	1
3.2.3.1.	Appropriations from voted budget.....	1
3.2.4.	Estimated requirements of human resources.....	1
3.2.4.1.	Financed from voted budget.....	2
3.2.5.	Overview of estimated impact on digital technology-related investments.....	4
3.2.6.	Compatibility with the current multiannual financial framework.....	5
3.2.7.	Third-party contributions	5
3.3.	Estimated impact on revenue	6
4.	Digital dimensions.....	6
4.1.	Requirements of digital relevance.....	6

1. FRAMEWORK OF THE PROPOSAL/INITIATIVE

1.1. Title of the proposal/initiative

Proposal for a Regulation of the European Parliament and Council on the European Union Critical Communication System (EUCCS).

1.2. Policy area(s) concerned

Internal security, civil protection, digital and space.

1.3. Objective(s)

1.3.1. General objective(s)

The general objective is to enhance Europe's capacity to react swiftly and effectively to incidents and crises that require response across borders and by cooperation of different types of emergency services.

1.3.2. Specific objective(s)

Specific objective No 1: Promote interoperable and secure cross-border and cross-agency/operator critical communication and operational mobility among emergency services.

The objective is to provide for emergency services a resilient critical communication infrastructure that enables seamless operational mobility promote interoperability and strengthen cross-border and cross-agency operational mobility for an enhanced emergency response . Specifically, all the critical communication systems of law enforcement, civil protection, and other emergency response services across Member States need to be harmonised and interconnected.

Specific objective No 2: Support Member States to deploy broadband critical communication systems.

The ability to exchange data-rich information, such as images or video, across borders and in real time was highlighted as a central reason for the upgrade of the current legacy systems used, notably TETRA. Most of the Member States report a planned upgrade of their national legacy narrowband systems.

There is no contradiction between the upgrade of narrowband systems and the transition to broadband. All critical communication systems in Member States will run for a certain time in a hybrid setting, in which TETRA and mission-critical broadband will run in parallel. This is called the 'migration phase' in which user groups shift step by step from TETRA to broadband networks. Member States may furthermore decide to run TETRA systems for longer periods to have a proven and widely available back-up solution for voice communication, which remains the single most important type of communication that must not fail during an emergency. It is important to underline that it is not EUCCS that 'replaces' TETRA. It is the

technological shift to broadband, that is already taking place, that will phase out narrowband technologies, like it has done already in commercial telecommunication. EUCCS is established therefore precisely at this moment in time, to use the ongoing, but still early transition towards mission-critical broadband to also introduce the interoperability requirement. EUCCS itself is agnostic to the possibility of Member States continue to run a narrowband system in parallel to their broadband system, on the condition that their hybrid solution allows for the interconnection with other Member States, covers the identified emergency services and offers the necessary functionalities. That is also why a ‘cut-off’ clause for narrowband systems (like the copper switch-off in the DNA) has not been considered.

Targeted interviews point to the need of transition to broadband to allow for the deployment of interoperable 5G mission-critical capabilities. Broadband communications technology satisfies the current and evolving needs for increasing data consumption, supporting advanced functionalities, such as real time incident reporting, high-resolution Geographic Information System (GIS), and high bandwidth data exchange (i.e., live video, biometric data), and facilitating the integration of Artificial Intelligence. In this regard, interviewees also underlined the role of harmonisation at technological level in making national investment in critical communications more attractive, while supporting the development of a more integrated and technologically advanced European critical communications ecosystem overall.

To conclude, a consensus is observed as to the necessity to transition to broadband as this would ensure that critical communication systems remain technologically robust, reliable, and future-proof, able to adapt to new technologies and develop new capabilities.

Specific objective No 3: Facilitate the achievement of a high and consistent level of resilience of critical communications across Member States.

Resilient infrastructure is needed to ensure connectivity and availability in all circumstances. In this context, resilience refers to the capacity of critical communication infrastructures to withstand, absorb, and rapidly recover from natural and man-made threats. Notably this can be achieved by ensuring advanced backup power, redundant coverage, separation of mission critical core network and radio access network as well as protocol and cryptographic security. In terms of security a broadband system would improve encryption and authentication allowing for stronger protection against cyberattacks. Resilient critical communication systems can thus be achieved by progressively strengthening the robustness of national critical communication systems through common resilience and security baselines and the deployment of advanced protective measures at EU level. Survey findings indicate that further action at the EU level would strengthen the overall resilience of national critical communication systems . Furthermore, achieving this specific objective would contribute to future-proofing critical communication systems,

increasing Europe's strategic autonomy in cases of geopolitical developments that harm EU interests.

1.3.3. *Expected result(s) and impact*

Specify the effects which the proposal/initiative should have on the beneficiaries/groups targeted.

Expected results

ER1: Enhanced operational mobility across borders and agencies for public authorities in charge of security and safety.

ER2: Increased resilience of Member States national critical communication system.

ER3: Increased operational efficiency Member States national critical communication system.

ER4: Progressive development and deployment of new or upgraded critical communication infrastructure, devices, applications and services, stimulating the continuous evolution of critical communication system.

ER5: National critical communication system can respond to evolving user needs and technological innovations.

Expected impacts:

EI1: Enhanced EU-wide preparedness and coordinated crisis response against natural or man-made disasters, terrorist and cross-border crimes, and armed conflicts through secure, reliable and interoperable critical communication systems that support coordinated action by all relevant emergency services.

EI2: Positive social impacts, including greater citizen trust, safety, security and civil protection across Member States enabled by faster, more coordinated and effective emergency responses, ultimately resulting in saving lives.

EI3: Positive environmental impacts, including earlier detection with faster and better coordinated cross-border responses to natural disasters, thereby reducing environmental damage.

1.3.4. *Indicators of performance*

Specify the indicators for monitoring progress and achievements.

The successful implementation of SO1 will be measured by the number of Member States that have interconnected critical communication systems, providing cross-border and inter-agency critical communication. This will be assessed in three stages: 2030, 2033, and 2036.

The successful implementation of SO2 would be measured by the number of Member States who deployed mission critical broadband systems as well as the total number of emergency services' personnel that are connected to those systems.

The successful implementation of SO3 would be measured by the compliance of Member States to the commonly agreed minimum resilience requirements.

To measure the success and effectiveness of the EUCCS, the below Key Performance Indicators have been identified, based on the EUCCS Operational Plan endorsed by the European Commission in May 2025. By monitoring these Key Performance Indicators, the European Commission can ensure that EUCCS will effectively meet its general objective: enhance Europe's capacity to react effectively and efficiently to cross-border and cross-agency incidents and crises, through a secure and resilient critical communication infrastructure across the EU and Schengen area.

1.4. The proposal/initiative relates to:

- ☐ a new action
- ☒ a new action following a pilot project / preparatory action⁵⁷
- ☐ the extension of an existing action
- ☐ a merger or redirection of one or more actions towards another/a new action

1.5. Grounds for the proposal/initiative

1.5.1. Requirement(s) to be met in the short or long term including a detailed timeline for roll-out of the implementation of the initiative

Following the principle of gradual establishment and by using leveraged maturity models like the ENISA CSIRT Maturity Assessment model and the CISA Zero Trust Maturity model, each Member State should gradually establish its mission-critical communication system by progressing through the below maturity levels and dimensions. Standardisation and certification, including on interoperability and security, will also play an important role in the different dimensions.

Each level should be understood as a target for each Member State to reach. Member States should establish their national mission-critical mobile broadband services capability from today's 'traditional' to 'initial' capability and evolve the maturity of its secure communication system towards 'optimal', progressing through all four maturity stages:

- Traditional – current
- Initial – to be achieved by 2030
- Advanced – to be achieved by 2033
- Optimal – to be achieved by 2036

The assessment of Member State's maturity of their national mission-critical communication system, regarding their maturity within the EUCCS, should be carried out by peer review by all Member States (via MCCG). The MCCG shall

⁵⁷

As referred to in Article 58(2), point (a) or (b) of the Financial Regulation.

follow jointly agreed criteria for the peer review. The concerned Member State submits evidence which is reviewed by all the other Member States.

- 1.5.2. *Added value of EU involvement (it may result from different factors, e.g. coordination gains, legal certainty, greater effectiveness or complementarities). For the purposes of this section 'added value of EU involvement' is the value resulting from EU action, that is additional to the value that would have been otherwise created by Member States alone.*

Reasons for action at EU level (ex-ante)

Over the past few years, Member States have experienced increasingly frequent and more severe natural and man-made disasters. Disasters such as the Covid-19 pandemic, catastrophic floods of July 2021 affecting Germany, Belgium and the Netherlands, the Iberian Peninsula blackout in April 2025, or the forest wildfires that took place throughout Europe in summer 2026. Crises affecting more than one Member State and requiring joint response are the new normal. Member States acknowledge thus the need for EU action: the Mission Critical Communication Group endorsed in 2025 the EUCCS Operational Plan to facilitate the task of coordinating the establishment of EUCCS. There are thus strong involvement and constant consultation with Member States, which requested action by the Commission on EUCCS, including by proposing a legal basis. Also in relevant Council working parties, as well as at the level of the Council itself, Member States had asked for the establishment of EUCCS for many years.

Furthermore, the study highlighted that one of the key challenges affecting the current situation of critical communications across the EU is the existence of varying levels of technological maturity of critical communication systems across the EU . Given that these systems evolve from different baselines, shaped by different budgetary capabilities, procurement cycles, and national risk appetite, the transition toward advanced technologies is progressing at an uneven pace.

Given that EUCCS will cover the whole of the EU and the Schengen area and will need to rely on a set of binding common rules, there is no realistic alternative to EU action. In the absence of such action, Member States would need to engage in a very large number of bilateral and multilateral agreements, operational procedures and technical arrangements, assuming they would still pursue the goal of interconnecting their next generation mission critical communication systems.

Expected generated EU added value (ex-post)

The Union's action can be considered more effective than what Member States acting alone can do, as it can establish a harmonised EU framework facilitating cross-border and interagency critical communications. Completing EUCCS for the whole of the EU and Schengen area by 2036 will directly benefit the operations of around five million members of emergency services in Europe to save lives and prevent harm to health and property, presenting one of the highest added values.

EUCCS will streamline the costly deployment of mission-critical broadband and thus create benefits for adequately planning of human and financial resources. Assuming all Member States are completing the transition to broadband by 2036, Member States remain responsible for covering the costs for their national systems. Several Member States (e.g. France, Finland) are currently allocating national funding for this purpose, using also EU funding such as the Recovery and Resilience Facility. Other Member States indicated in the Mission Critical Communication Group that they would seek EU financial support to transition to mission critical broadband. Such funding could easier be part of the future EU funding programmes, if it corresponded to a legal obligation.

When measuring the added value of EU action, it is important to consider that the technical basis for EUCCS is the result of cooperation of the Commission, Member States and European industry. The components of the system have been developed and tested by Member States' stakeholders, notably around 100 emergency services to validate that the solution creates added value.

1.5.3. *Lessons learned from similar experiences in the past*

The EU-funded project Inter System Interoperability for TETRA-TetraPol Networks (ISITEP), developed a cross-border communication infrastructure based on IP integration. It was not further pursued for logistical, budgetary and operational reasons. Furthermore, there have been previous attempts at connecting TETRA systems, but only the Nordic countries - Norway, Sweden and Finland - succeeded in integrating their networks in the Inter-System Interface (ISI)⁵⁸. Attempts to replicate the Nordic success at EU-level did not yield tangible results⁵⁹.

The Regulation is based on more than 10 years of EU-funded research. BroadMap and BroadWay projects (2016 – 2022) was based on a voluntary approach that should lead to a coordinated procurement of inter-operable solutions. The project led to the common understanding of Member States and the Commission services that only an approach based on binding EU-level rules is likely to successfully establish EUCCS.

1.5.4. *Compatibility with the multiannual financial framework and possible synergies with other appropriate instruments*

Without prejudice to the outcome of the negotiations on the next Multiannual financial framework (MFF) the proposal, may be supported by Union programmes in accordance with the objectives set out in the regulations establishing those funds and programmes. The LFDS presents estimated budgetary impact under Heading 4 including related human and administrative resources.

⁵⁸ [Norway and Sweden Interconnect Secure Radio Communication Networks - TCCA.](#)

⁵⁹ However, many of the key lessons have been translated into EUCCS via the EUCCS Preparation Project, which included since its start experts from ISI. Notably the need to supplement technical interoperability with Operational Procedures and to set up a governance for the system to function are lessons-learnt from the Nordics. The same is true for the experience of international partners, notably the U.S. FirstNet.

1.5.5. *Assessment of the different available financing options, including scope for redeployment*

Without prejudice to the outcome of the negotiations on the next Multiannual financial framework (MFF) the proposal, may be supported by Union programmes in accordance with the objectives set out in the regulations establishing those funds and programmes. The LFDS presents estimated budgetary impact under Heading 4 including related human and administrative resources.

1.6. Duration of the proposal/initiative and of its financial impact

☐ limited duration

- ☐ in effect from [DD/MM]YYYY to [DD/MM]YYYY
- ☐ financial impact from YYYY to YYYY for commitment appropriations and from YYYY to YYYY for payment appropriations.

☒ unlimited duration

- Implementation with a start-up period from 2030,
- followed by full-scale operation.

1.7. Method(s) of budget implementation planned⁶⁰

☐ Direct management by the Commission

- ☐ by its departments, including by its staff in the Union delegations;
- ☐ by the executive agencies

☐ Shared management with the Member States

☐ Indirect management by entrusting budget implementation tasks to:

- ☐ third countries or the bodies they have designated
- ☐ international organisations and their agencies (to be specified)
- ☐ the European Investment Bank and the European Investment Fund
- ☐ bodies referred to in Articles 70 and 71 of the Financial Regulation
- ☐ public law bodies
- ☐ bodies governed by private law with a public service mission to the extent that they are provided with adequate financial guarantees
- ☐ bodies governed by the private law of a Member State that are entrusted with the implementation of a public-private partnership and that are provided with adequate financial guarantees
- ☐ bodies or persons entrusted with the implementation of specific actions in the common foreign and security policy pursuant to Title V of the Treaty on European Union, and identified in the relevant basic act
- ☐ bodies established in a Member State, governed by the private law of a Member State or Union law and eligible to be entrusted, in accordance with sector-specific rules, with the implementation of Union funds or budgetary guarantees, to the extent that such bodies are controlled by public law bodies or by bodies governed by private law with a public service mission, and are provided with adequate financial guarantees in the form of joint and several liability by the

⁶⁰ Details of budget implementation methods and references to the Financial Regulation may be found on the BUDGpedia site: <https://myintracomm.ec.europa.eu/corp/budget/financial-rules/budget-implementation/Pages/implementation-methods.aspx>.

controlling bodies or equivalent financial guarantees and which may be, for each action, limited to the maximum amount of the Union support.

Comments

The funding indicated for the EUCCS European components and the Member States' interconnection component will be directly managed by the Commission.

The methods of budget implementation of the sources of financing and scope of Union financial commitment in the post-2027 period remain subject to the outcome of interinstitutional negotiations on the MFF 2028-2034

2. MANAGEMENT MEASURES

2.1. Monitoring and reporting rules

This Regulation will establish a System Accreditation Board comprising of delegates from Member States to assess the progressive maturity of national critical communication systems in line with the EUCCS, including notably if a Member State is ready to join EUCCS. It would build on the EUCCS maturity approach (Traditional → Initial 2030 → Advanced 2033 → Optimal 2036) . Its activities would cover the verification of national critical communication systems interconnection, roaming readiness, rollout of baseline mission critical services and key enabling capabilities, as well as alignment with the EUCCS security and resilience expectations, notably recognised cybersecurity management practices and the progressive uptake of European Telecommunications Standards Institute/Global Certification Forum standardisation and certification . Maturity assessment would be conducted through a structured peer-review process using objective and proportionate criteria and evidence, ensuring comparability. For legal reasons, the function of the System Accreditation Board cannot be performed by the European Union Critical Communication Group (or any other comitology committee).

A Member State critical communication system is accredited by the System Accreditation Board. The Commission should organise a monitoring mission to assess the compliance with the obligations set out in this Regulation. In duly justified cases, the Board may also request the Commission to organise a monitoring mission to one or several Member States whose critical communication system have been already accredited to verify continuous compliance.

Each monitoring mission shall consist of experts from the Member State in which the critical communication system is located, experts from other Member States and Commission representatives. Additional experts, including from EU Agencies or bodies, may be nominated as observers to join a mission.

The Commission shall, following a consultation with the Member State that operates the critical communication system, select and appoint the members of each monitoring mission in accordance with their professional capacity.

The Commission should inform the European Union Critical Communication Group of the organisation of a monitoring mission.

Furthermore, relevant Regulation(s) related to the MFF 2028-2034 will applied.

2.2. Management and control system(s)

2.2.1. *Justification of the budget implementation method(s), the funding implementation mechanism(s), the payment modalities and the control strategy proposed*

By five years after the entry into force of this Regulation, and every five years thereafter, the Commission should submit a report to the European Parliament and to the Council on the implementation of this Regulation, including detailed information

on how each Member State has implemented it, and should, where appropriate, propose amendments to this Regulation.

Similarly, the Member States should, at the request of the Commission, provide it with the information necessary for the preparation of the report no later than nine months before the expiry of the reporting deadline.

Concerning the management and control systems, relevant provisions related to the MFF 2028-2034 will be applied.

2.2.2. *Information concerning the risks identified and the internal control system(s) set up to mitigate them*

Concerning management and control systems, relevant provisions related to the MFF 2028-2034 will be applied.

2.2.3. *Estimation and justification of the cost-effectiveness of the controls (ratio between the control costs and the value of the related funds managed), and assessment of the expected levels of risk of error (at payment & at closure)*

Concerning management and control systems, relevant provisions related to the MFF 2028-2034 will be applied.

2.3. Measures to prevent fraud and irregularities

The existing fraud preventive measures applicable to the Commission will cover the appropriations necessary for this Regulation. Concerning prevention of fraud and irregularities, relevant provisions related to the MFF 2028-2034 will be applied.

3. ESTIMATED FINANCIAL IMPACT OF THE PROPOSAL/INITIATIVE

The estimated impact on expenditure and staffing for 2028 and beyond is added for illustrative purposes only and does not pre-judge the next Multiannual Financial Framework. The source of financing and scope of Union financial commitment in the post-2027 period remain subject to the outcome of interinstitutional negotiations on the MFF 2028-2034 and thereafter shall be determined through the annual budgetary procedure. All appropriations and staffing allocations as of 2028 are indicative.

3.1. Heading(s) of the multiannual financial framework and expenditure budget line(s) affected

- Existing budget lines

In order of multiannual financial framework headings and budget lines.

Heading of multiannual financial framework	Budget line	Type of expenditure	Contribution			
	Number	Diff./Non-diff. ⁶¹	from EFTA countries ⁶²	from candidate countries and potential candidates ⁶³	From other third countries	other assigned revenue

			Contribution			

⁶¹ Diff. = Differentiated appropriations / Non-diff. = Non-differentiated appropriations.

⁶² EFTA: European Free Trade Association.

⁶³ Candidate countries and, where applicable, potential candidates from the Western Balkans.

3.2. Estimated financial impact of the proposal on appropriations

3.2.1. Summary of estimated impact on operational appropriations

- ☐ The proposal/initiative does not require the use of operational appropriations
- ☒ The proposal/initiative requires the use of operational appropriations, as explained below

3.2.1.1. Appropriations from voted budget

EUR million (to three decimal places)

Heading of multiannual financial framework			Number	TBC						
DG: HOME			Year	Year	Year	Year	Year	Year	Year	TOTAL MFF 2028-2034
			2028	2029	2030	2031	2032	2033	2034	
Operational appropriations										
Budget line	Commitments	(1a)	p.m.	p.m.	p.m	p.m	p.m	p.m	p.m	p.m
	Payments	(2a)	p.m.	p.m	p.m	p.m	p.m	p.m	p.m	p.m
Budget line	Commitments	(1b)								0
	Payments	(2b)								0
Appropriations of an administrative nature financed from the envelope of specific programmes ⁶⁴										
Budget line		(3)	0	0	0	0	0	0	0	0
TOTAL appropriations	Commitments	=1a+1b+3	p.m	p.m	p.m	p.m	p.m	p.m	p.m	p.m

⁶⁴ Technical and/or administrative assistance and expenditure in support of the implementation of EU programmes and/or actions (former 'BA' lines), indirect research, direct research.

for DG <HOME ⁶⁵ >		Payments	=2a+2b+3		p.m	p.m	p.m	p.m	p.m	p.m					p.m
						(									

						1				

Heading of multiannual financial framework	4	‘Administrative expenditure’ ⁶⁶
---	---	--

DG: <HOME>		Year 2028	Year 2029	Year 2030	Year 2031	Year 2032	Year 2033	Year 2034	TOTAL MFF 2028- 2034
Y Human resources		1.202	1.202	1.202	1.202	1.202	1.202	1.202	8.414
Y Other administrative expenditure		0.620	0.870	0.870	1.120	0.870	0.870	1.120	6.340
TOTAL DG <HOME>		1.822	2.072	2.072	2.322	2.072	2.072	2.322	14.754

⁶⁶ The necessary appropriations should be determined using the annual average cost figures available on the appropriate BUDGpedia webpage.

DG: <DIGIT>		Year 2028	Year 2029	Year 2030	Year 2031	Year 2032	Year 2033	Year 2034	TOTAL MFF 2028- 2034
Y Human resources		0.388	0.388	0.388	0.388	0.388	0.388	0.388	2.716
Y Other administrative expenditure		0	0	0	0	0	0	0	0
TOTAL DG <DIGIT>	Appropriations	0.388	0.388	0.388	0.388	0.388	0.388	0.388	2.716

TOTAL appropriations under HEADING 4 of the multiannual financial framework	(Total commitments = Total payments)	2.210	2.460	2.460	2.710	2.460	2.460	2.710	17.470
--	---	--------------	--------------	--------------	--------------	--------------	--------------	--------------	---------------

The estimated impact on expenditure and staffing for 2028 and beyond is added for illustrative purposes only and does not pre-judge the next Multiannual Financial Framework. The source of financing and scope of Union financial commitment in the post-2027 period remain subject to

the outcome of interinstitutional negotiations on the MFF 2028-2034 and thereafter shall be determined through the annual budgetary procedure.
All appropriations and staffing allocations as of 2028 are indicative

				t													

-																	
- Output																	
- Output																	

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

3.2.3. Summary of estimated impact on administrative appropriations

- ☐ The proposal/initiative does not require the use of appropriations of an administrative nature
- ☒ The proposal/initiative requires the use of appropriations of an administrative nature, as explained below

3.2.3.1. Appropriations from voted budget

VOTED APPROPRIATIONS	Year	Year	Year	Year	Year	Year	Year	TOTAL 2028 - 2034
	2028	2029	2030	2031	2032	2033	2034	
HEADING 4								
Human resources	1.590	1.590	1.590	1.590	1.590	1.590	1.590	11.130
Other administrative expenditure	0.620	0.870	0.870	1.120	0.870	0.870	1.120	6.34
TotalHEADING 4	2.210	2.460	2.460	2.710	2.460	2.460	2.710	17.470
Outside HEADING 4								

The estimated impact on expenditure and staffing for 2028 and beyond is added for illustrative purposes only and does not pre-judge the next Multiannual Financial Framework. The source of financing and scope of Union financial commitment in the post-2027 period remain subject to the outcome of interinstitutional negotiations on the MFF 2028-2034 and thereafter shall be determined through the annual budgetary procedure. All appropriations and staffing allocations as of 2028 are indicative.

3.2.4. Estimated requirements of human resources

- ☐ The proposal/initiative does not require the use of human resources
- ☒ The proposal/initiative requires the use of human resources, as explained below

3.2.4.1. Financed from voted budget

Estimate to be expressed in full-time equivalent units (FTEs)⁶⁷

VOTED APPROPRIATIONS		Year 2028	Year 2029	Year 2030	Year 2031	Year 2032	Year 2033	Year 2034
• Establishment plan posts (officials and temporary staff)								
20 01 02 01 (Headquarters and Commission's Representation Offices)		6	6	6	6	6	6	6
20 01 02 03 (EU Delegations)		0	0	0	0	0	0	0
(Indirect research)		0	0	0	0	0	0	0
(Direct research)		0	0	0	0	0	0	0
Other budget lines (specify)		0	0	0	0	0	0	0
• External staff (inFTEs)								
20 02 01 (AC, END from the 'global envelope')		4	4	4	4	4	4	4
20 02 03 (AC, AL, END and JPD in the EU Delegations)		0	0	0	0	0	0	0
Admin. Support line [XX.01.YY.YY]	• at Headquarters	0	0	0	0	0	0	0
	• in EU Delegations	0	0	0	0	0	0	0
(AC, END - Indirect research)		0	0	0	0	0	0	0
(AC, END - Direct research)		0	0	0	0	0	0	0
Other budget lines (specify) - Heading 4		0	0	0	0	0	0	0
Other budget lines (specify) - Outside Heading 4		0	0	0	0	0	0	0
TOTAL		10	10	10	10	10	10	10

⁶⁷ Please specify below the table how many FTEs within the number indicated are already assigned to the management of the action and/or can be redeployed within your DG and what are your net needs.

The estimated impact on expenditure and staffing for 2028 and beyond is added for illustrative purposes only and does not pre-judge the next Multiannual Financial Framework. The source of financing and scope of Union financial commitment in the post-2027 period remain subject to the outcome of interinstitutional negotiations on the MFF 2028-2034 and thereafter shall be determined through the annual budgetary procedure. All appropriations and staffing allocations as of 2028 are indicative.

The staff required to implement the proposal (in FTEs):

	To be covered by current staff available in the Commission services	Exceptional additional staff*		
		To be financed under Heading 4 or Research	To be financed from BA line	To be financed from fees
Establishment plan posts	6 (5 AD and 1 AST posts)		N/A	
External staff (CA, SNEs, INT)	4 (2 CA and 2 END)			

Description of tasks to be carried out by:

Officials and temporary staff	DG HOME (3 AD and 1 AST posts): Overall implementation of the EUCCS at national and EU level, including management of the European Union Critical Communication Group and the System Accreditation Board. Preparation and adoption of implementing and delegated acts. DG DIGIT (2 AD): Support to the establishment of the mission-critical interconnection infrastructure. Establishment and operation of the European Network Monitoring Centre and of the European Security Monitoring Centre.
-------------------------------	--

External staff	DG HOME (2 CA and 2 END): Support to the overall implementation of the EUCCS at national and EU level, including management of the European Union Critical Communication Group and the System Accreditation Board. Preparation and adoption of implementing and delegated acts.

The estimated impact on expenditure and staffing for 2028 and beyond is added for illustrative purposes only and does not pre-judge the next Multiannual Financial Framework. The source of financing and scope of Union financial commitment in the post-2027 period remain subject to the outcome of interinstitutional negotiations on the MFF 2028-2034 and thereafter shall be determined through the annual budgetary procedure. All appropriations and staffing allocations as of 2028 are indicative.

3.2.5. *Overview of estimated impact on digital technology-related investments*

Compulsory: the best estimate of the digital technology-related investments entailed by the proposal/initiative should be included in the table below.

Exceptionally, when required for the implementation of the proposal/initiative, the appropriations under Heading 4 should be presented in the designated line.

The appropriations under Headings 1-3 should be reflected as “Policy IT expenditure on operational programmes”. This expenditure refers to the operational budget to be used to re-use/ buy/ develop IT platforms/ tools directly linked to the implementation of the initiative and their associated investments (e.g. licences, studies, data storage etc). The information provided in this table should be consistent with details presented under Section 4 “Digital dimensions”.

TOTAL Digital and IT appropriations	Year 2028	Year 2029	Year 2030	Year 2031	Year 2032	Year 2033	Year 2034	TOTAL MFF 2028 - 2034
HEADING 4								

IT expenditure (corporate)	0	0	0	0	0	0	0	0
Subtotal HEADING 4	0	0	0	0	0	0	0	0

3.2.6. *Compatibility with the current multiannual financial framework*

The proposal/initiative:

- ☐ can be fully financed through redeployment within the relevant heading of the multiannual financial framework (MFF)
- ☐ requires use of the unallocated margin under the relevant heading of the MFF and/or use of the special instruments as defined in the MFF Regulation
- Without prejudice to the outcome of the negotiations on the next Multiannual Financial Framework (MFF) the proposal may be supported by Union programmes in accordance with the objectives set out in the regulations establishing those funds and programmes. ☐ requires a revision of the MFF

3.2.7. *Third-party contributions*

The proposal/initiative:

- ☐ does not provide for co-financing by third parties
- ☐ provides for the co-financing by third parties estimated below:

Appropriations in EUR million (to three decimal places)

	Year 2028	Year 2029	Year 2030	Year 2031	Year 2032	Year 2033	Year 2034	Total
Specify the co-financing body								
TOTAL appropriations co-financed								

3.3. Estimated impact on revenue

- ☐ The proposal/initiative has no financial impact on revenue.
- ☐ The proposal/initiative has the following financial impact:
 - ☐ on own resources
 - ☐ on other revenue
 - ☐ please indicate, if the revenue is assigned to expenditure lines

EUR million (to three decimal places)

Budget revenue line:	Appropriations available for the current financial year	Impact of the proposal/initiative ⁶⁸						
		Year 2028	Year 2029	Year 2030	Year 2031	Year 2032	Year 2033	Year 2034
Article								

For assigned revenue, specify the budget expenditure line(s) affected.

Other remarks (e.g. method/formula used for calculating the impact on revenue or any other information).

4. DIGITAL DIMENSIONS

4.1. Requirements of digital relevance

High-level description of the requirements of digital relevance and related categories (data, process digitalisation & automation, digital solutions and/or digital public services)

⁶⁸ In the case of traditional own resources (customs duties, sugar levies), the amounts indicated must be net amounts, i.e. gross amounts after deduction of 10 % for collection costs, as proposed in COM(2025)574.

Reference to the requirement	Requirement description	Actors affected or concerned by the requirement	High-level Processes	Categories
Article 1	Establishes the EU Critical Communication System (EUCCS).	European Commission, Member States		Digital solution Digital public service
Article 2	Member States shall ensure that their national critical communication systems used by competent law enforcement authorities are interoperable so that they can be interconnected at Union level.	European Commission, Member States		Digital solution Digital public service
Article 4	Each Member State to designate a competent authority; for competent authorities to cooperate where possible.	Member States		Digital public service Data
Article 5	Member State shall adopt and transmit to the Commission a critical communication strategy.	European Commission, Member States		Data
Article 6	Minimum requirements for components of a Member State's critical communication system	Member States		Digital solution Digital public service
Article 7	Member States shall take the necessary measures to ensure the resilience of all components of critical communication systems. The Commission is empowered to	European Commission, Member States		Digital solution

	adopt an implementing acts establishing minimum requirements for the security and resilience of the Member States' critical communication systems.			
Article 8	Member States shall ensure the availability of public electronic communications networks to convey critical communications with the level of quality required to ensure its uninterrupted availability and effective functioning, including in emergency and crisis situations subject to the relevant commercial agreements with providers of such public electronic communication services.	Member States, providers of public electronic networks		Data
Article 9 Article 10	Establishment of a European Union Critical Communication Group and a System Accreditation Board	European Commission, Member States		Digital public service
Article 11	To be accredited, Member States' systems must comply with relevant European/International standards and specifications. Must ensure interoperability, security, resilience, and the proper functioning. The Commission may adopt delegated acts to this effect.	European Commission, Member States, standardisation bodies		Digital solution Digital public service

Article 13	Detailing the interconnection of Member States' critical communication systems. The Commission shall make available a Critical Communication Interconnection infrastructure that facilitates the interconnection of Member States' systems.	European Commission, Member States		Digital solution Digital public service
Article 14	Interconnection of Member States' systems to the System shall be implemented in three stages.	European Commission, Member States		Digital public service
Article 15 Article 16	The Commission shall establish: a European Union Network Monitoring Centre; a European Union Security Monitoring Centre.	European Commission,		Digital public service Data
Article 17	The Commission shall adopt an implementing act to lay down standard operating procedures for the Member States' competent authorities and emergency services for the consistent, efficient, and compliant use of the System.	European Commission		Digital public service
Article 18	Requirements as to the use of EU Satellite Secure Connectivity services	European Commission, Member States		Digital public service Digital solution
Article 19	The Commission shall support the	European Commission,		Digital public service

	coordination of Member States' technical and operational cooperation on critical communication.	Member States		
Article 20	Evaluations	European Commission		Data

4.2. Data

High-level description of the data in scope

Type of data	Reference to the requirement(s)	Standard and/or specification (if applicable)
Designation of competent authorities	Article 4	—
Mission-critical broadband communication strategy	Article 5	—
Communications conveyed over public electronic communication networks	Article 8	Of required quality, including with regard to parameters such as latency, jitter, packet loss, and throughput
Report from the European Union Network Monitoring Centre	Article 15	—
Information collected and aggregated by the European Union Security Monitoring Centre	Article 16	
Reports by the European Union Security Monitoring Centre (issue recommendations, propose mitigation measures or suggest corrective actions)	Article 16	
Reports from the European Union Security Monitoring Centre concerning security incidents, vulnerabilities, and risks	Article 16	

Critical incident notifications	Article 16	
Security evidence to be used for system accreditation purposes	Article 16	
Reports by the European Union Security Monitoring Centre following a critical incident	Article 16	
Report on the implementation of this Regulation	Article 20	—
Information provided for the purpose of preparing an evaluation report	Article 20	—

Alignment with the European Data Strategy

The EUCCS aligns with the European Data Strategy, as it is developed designed to put people first, uphold European values, and make more data available for protectiong our societies.

The EUCCS aligns with the General Data Protection Regulation (GDPR).

Alignment with the once-only principle

The EUCCS aligns with the once-only principle. The data remains with the Member States which will store, secure and reuse them following the GDPR. Newly create data is accessible, interoperable and meets high-quality standards, facilitating the delivery of timely and efficient crisis response across the European Union.

Data flows

High-level description of the data flows

Type of data	Reference(s) to the requirement(s)	Actors who provide the data	Actors who receive the data	Trigger for the data exchange	Frequency (if applicable)
Designation of competent authorities	Article 4	Member States	European Commission	Competent authority designated (no later than three months after the entry into force of this Regulation)	//
Mission-critical broadband communication strategy	Article 5	Member States	European Commission	Member State shall adopt and transmit to the Commission a critical communication strategy. That strategy shall set out the measures required for the transition from existing narrowband to broadband and packet switched critical communication, as well as for the interconnection of the critical communication system of the Member State to the systems of other Member States	Member States shall regularly review and, where appropriate, update their critical communication strategies and communicate any updates to the Commission upon their adoption.
Communications conveyed over public electronic communication networks	Article 8	public electronic networks	Member States	Member States shall ensure the availability of public electronic communications networks to convey critical communications with the level of quality required to	

				ensure its uninterrupted availability and effective functioning, including in emergency and crisis situations subject to the relevant commercial agreements with providers of such public electronic communication services. Such level of quality shall take into account relevant technical parameters, including latency, jitter, packet loss and throughput.	
Report from the European Union Network Monitoring Centre	Article 15	European Union Network Monitoring Centre	European Commission	The European Network Monitoring Centre shall cooperate closely with the European Security Monitoring Centre and shall provide it, without undue delay, with network events, performance information and other operational data necessary for cybersecurity monitoring, incident detection and response.	
Information collected and aggregated by the European Union Security Monitoring Centre	Article 16	Member States Critical Communication Security	European Union Security Monitoring Centre	The Member States' Critical Communication Security Operations Centres as referred to in Article 7 shall provide reports on a regular	

		Operations Centres		basis concerning security incidents, vulnerabilities and risks affecting the System to the European Security Monitoring Centre	
Reports by the European Security Monitoring Centre (issue recommendations, propose mitigation measures or suggest corrective actions)	Article 16	European Union Security Monitoring Centre	European Commission	The European Security Monitoring Centre shall issue recommendations, propose mitigation measures or suggest corrective actions concerning security incidents, vulnerabilities and risks affecting Union-level critical communication roaming, communication infrastructure, users' authentication and mission-critical service interoperability	
Reports from the European Security Monitoring Centre concerning security incidents, vulnerabilities, and risks	Article 16	European Union Security Monitoring Centre	European Commission	In case of a critical incident as referred to in paragraph 1, it shall provide a report without undue delay. It shall cooperate with the Member States' competent authorities and cybersecurity authorities, CSIRTs Network members and relevant Union bodies and agencies to manage incidents and to follow-up on recommendations and corrective actions.	

Critical incident notifications	Article 16	European Union Security Monitoring Centre	European Commission	In case of a critical incident as referred to in paragraph 1, it shall provide a report without undue delay. It shall cooperate with the Member States' competent authorities and cybersecurity authorities, CSIRTs Network members and relevant Union bodies and agencies to manage incidents and to follow-up on recommendations and corrective actions.	
Security evidence to be used for system accreditation purposes	Article 16	European Union Security Monitoring Centre	European Commission	The European Security Monitoring Centre shall support testing of security controls for roaming authentication and authorisation, trust management, interconnection interfaces and mission-critical service interoperability	
Reports by the European Security Monitoring Centre following a critical incident	Article 16	Member States Critical Communication Security Operations Centres	European Union Security Monitoring Centre	A Critical Communication Security Operations Centre shall notify any incident that interferes with or interrupts the functioning of the national critical communications system or of its interconnection ('critical incident') to the European Security Monitoring Centre	

				without delay and latest within [48 hours] of the discovery of the incident.	
Report on the implementation of this Regulation	Article 20	European Commission	European Parliament and to the Council	The Commission shall submit a report to the European Parliament and to the Council on the implementation of this Regulation, including detailed information on how each Member State has implemented it, and shall, where appropriate, propose amendments to this Regulation.	By five years after the entry into force of this Regulation, and every five years thereafter
Information provided for the purpose of preparing an evaluation report	Article 20	Member States	European Commission	Member States shall, at the request of the Commission, provide it with the information necessary for the preparation of the report referred to in paragraph 1, no later than nine months before the expiry of the reporting deadline.	

4.3. Digital solutions

High-level description of digital solutions

Digital solution	Reference(s) to the requirement(s)	Main mandated functionalities	Responsible body	How is accessibility catered for?	How is reusability considered?	Use of AI technologies (if applicable)
EU Critical Communications System (Interconnection via the Mission Critical Interconnection infrastructure)	Article 1 Article 11 Article 13 Article 14 Article 19	The EU Critical Communications System will interconnect the MS' critical communication systems at the EU level (connectivity for emergency services). Secure, sovereign Mission Critical Interconnection infrastructure that facilitates the interconnection of Member States' systems. This shall: • Provide connectivity dedicated to communications and information exchange between MSs' critical communication systems – Ensure confidentiality, integrity, availability – Be designed to remain operational and performant, incl. during crises affecting the public network. Where authorised by the GOVSATCOM and IRIS² Competent Authorities (CGA), users and devices of the System shall have access to secure satellite connectivity services provided under: (a) GOVSATCOM, as established by Regulation (EU) 2021/696; and (b) IRIS², as established by Regulation (EU) 2023/588.	European Commission			N/A

Member States' critical communication systems	Article 6 Article 7 Article 11 Article 12	Shall comprise de minimis: Radio Access Network; Critical Communication Core; Mission Critical Services. Must comply with relevant European/International standards and specifications. Ensure interoperability, security, resilience, proper functioning.	Member States			N/A
---	--	---	---------------	--	--	-----

For each digital solution, explanation of how the digital solution complies with applicable digital policies and legislative enactments

EU Critical Communications System (Interconnection via the Mission Critical Interconnection infrastructure)

Digital and/or sectorial policy (when these are applicable)	Explanation on how it aligns
<i>AI Act</i>	Aspects to be further developed in implementing/delegated acts
<i>EU Cybersecurity framework</i>	Limiting and prohibiting the use of equipment from high-risk suppliers, especially those subject to intrusive third-country laws regarding national intelligence and data security. Art. 7 - ensure the sovereignty, the exclusion of high-risk suppliers and overall supply chain security related to at least the Critical Communication Core, in alignment with the Cybersecurity Act 2 (CSA2)
<i>eIDAS</i>	Aspects to be further developed in implementing/delegated acts
<i>Single Digital Gateway and IMI</i>	Aspects to be further developed in implementing/delegated acts
<i>Others</i>	

Member States' critical communication systems

Digital and/or sectorial policy (when these are applicable)	Explanation on how it aligns
<i>AI Act</i>	Aspects to be further developed in implementing/delegated acts
<i>EU Cybersecurity framework</i>	Article 7: reference made to Directive (EU) 2022/2557 (Critical Entities Resilience Directive) and Directive (EU) 2022/2555 (NIS2). The Commission is empowered to adopt an Implementing Act to further specify minimum requirements for the security and resilience.
<i>eIDAS</i>	Aspects to be further developed in implementing/delegated acts
<i>Single Digital Gateway and IMI</i>	Aspects to be further developed in implementing/delegated acts
<i>Others</i>	

4.4. Interoperability assessment

High-level description of the digital public service(s) affected by the requirements

Digital public service or category of digital public services	Description	Reference(s) to the requirement(s)	Interoperable Europe Solution(s)	Other interoperability solution(s)
Cross-border and cross-agency critical communication (EU Critical Communications System)	Interconnection of Member States' systems will be facilitated, and a central EU level monitoring capacity will be established. The combination of those elements is the EU-level component of the EU Critical Communication System (EUCCS). It will be created an EU-level technical and	Article 1 Article 2 Article 4 Article 6 Article 11 Article 12	N/A	N/A

	component that provides the initial interconnection functionality for the Member States' systems and ensures high-level monitoring of the Member State networks. EUCCS is expected to have a high impact on digitalisation of Public Administration and promote broadband deployment. Critical communication among emergency services and other relevant forces will contribute to digitalisation of their operations. It will also contribute to Digital Government goals, including interoperability of Public Services.	Article 14 Article 15 Article 16 Article 17 Article 18 Article 19		
--	--	---	--	--

Impact of the requirement(s) as per digital public service on cross-border interoperability

Cross-border and cross-agency critical communication

Assessment	Measure(s)	Potential remaining barriers (if applicable)
Alignment with existing digital and sectorial policies	This Regulation is ensuring consistency with existing and forthcoming EU initiatives (e.g., NIS2, the 5G Cybersecurity Toolbox, EU ICT Supply Chain Security Toolbox).	—
Organisational measures for a smooth cross-border digital public services delivery	This Regulation will establish a governance architecture to ensure coordinated implementation, consistent decision-making, and clear accountability. More specifically:	

Please list the governance measures foreseen	– Each Member States would retain jurisdiction and operational control over its infrastructure and servers. At the same time, interconnection would be mandatory to guarantee operational mobility and seamless cross-border communications. (Article 1; Article 12) – Member States must connect their national critical communication systems within a defined transition period. (Article 14) • Designation of a National Competent Authority as the Member States' EUCCS single point of contact. The National Competent Authority would oversee the development, implementation, and operation of national mission critical broadband system and services, ensure security and resilience, and enable interoperability and cross-border cooperation, including EUCCS testing, field exercises, and reporting processes. Each National Competent Authority would need to appoint a Single Point of Contact for coordination with other National Competent Authorities. (Article 4) • Member States must prepare a mission-critical broadband communication strategy. This will set out measures to establish a (national) critical communication system; to realise the transition from existing narrowband/analogue communication systems to mission-critical broadband; the interconnection into the System. (Article 5) • Establishment of a European Union Critical Communication Group whose tasks include providing strategic guidance on the establishment and further development of System and Member States' systems components. (Article 9) • Framework for the accreditation of Member States' systems. A System Accreditation Board will be established to accredit the readiness for inclusion of Member States' systems into the	
--	--	--

	EUCCS based on the maturity levels detailed in the Annex to this Regulation. Member States will be required to pursue accreditation by making a request to the Board. (Article 10, Article 12) • A European Network Monitoring Centre will be established. This will operate an IP interconnection exchange to facilitate interconnection of critical communication systems and monitoring of transmission capabilities. (Article 15) • A European Security Monitoring Centre will be created to receive and review reports and issue recommendations or corrective actions on security incidents that affect Member States' critical communication systems. It does not handle security incidents itself but acts as monitoring capacity. Following good practice from the telecommunication sector and related policy domains, the Network Monitoring Centre and Security Monitoring Centre are going to be separate entities. They will be set up by the European Commission, likely using framework contracts to designate a specialised commercial service provider. (Article 16) • The Commission shall adopt an implementing act to lay down standard operating procedures for the Member States' competent authorities and emergency services for the consistent, efficient, and compliant use of the System. The standard operating procedures shall lay down the roles, tasks, coordination mechanisms, and protocols needed for the operational use of the System. They shall also cover elements with regard to cross-border communication between different types of emergency services. (Article 17) • The Commission shall support the coordination of Member States' technical and operational cooperation on critical communication. (Article 19)	
Measures taken to ensure a shared	//	

understanding of the data		
Use of commonly agreed open technical specifications and standards	<u>System Interconnections</u> – Member States shall ensure that Frontex and Europol and the European Union Customs Authority is granted access to use the EUCCS. (Article 2) – Each Member State shall ensure that its mission-critical broadband communication system is able to interconnect with the systems of other Member States. (Article 6) – Once the systems are accredited by the System Accreditation Board, Member States shall ensure the interconnection of their national systems with the EUCCS via the Mission Critical Interconnection infrastructure (Article 11, 13 14). — <u>Standards and Specifications</u> Interconnection would be based on common standards and agreed technical profiles to ensure end-to-end interoperability verified prior to connection to the EUCCS against conformance testbeds hosted by the European Network Monitoring Centre. The testing would verify technical, operational, and administrative conformance of the connected national critical communication systems against the established standards. The Commission may adopt delegated acts to establish a list or relevant standards and technical specifications. (Article 11; Article 17) <u>Mission Critical Interconnection infrastructure (Article 13)</u> The Commission shall make available a secure, sovereign, Mission Critical Interconnection infrastructure that facilitates the interconnection of Member States’ systems. This will provide connectivity dedicated to communications and information exchange between Member States’	

	critical communication systems.	
	<u>Use of EU Satellite Secure Connectivity services (Article 18)</u> As concerning access to secure satellite connectivity services provided under GOVSATCOM and IRIS², Member State competent authorities shall ensure the availability, interoperability, and effective use of secure satellite connectivity services within national critical communication systems.	

4.5. Measures to support digital implementation

High-level description of measures supporting digital implementation

Description of the measure	Reference(s) to the requirement(s)	Commission role (if applicable)	Actors to be involved (if applicable)	Expected timeline (if applicable)
Member States will adopt and maintain an EUCCS strategy/roadmap aligned with the EU legislative act and the EUCCS Operational Plan.	Article 5		Member States	
The Commission is empowered to adopt an Implementing Act to further specify minimum requirements for the security and resilience of Member States' critical communication systems.	Article 7	Adopt an Implementing Act	European Commission	

The Commission may adopt delegated acts to establish a list of relevant standards and technical specifications that Member States' systems must comply with.	Article 11	Adopt Delegated Act	Member States, standardisation bodies	
The Commission shall adopt implementing acts as relating to the use of EU Satellite Secure Connectivity services	Article 18	Adopt an Implementing Act	GOVSATCOM and IRIS ² Competent Authorities	

