ANALYSIS REPORT ON THE REGULATORY IMPACT OF THE DRAFT ROYAL DECREE APPROVING THE NATIONAL 5G NETWORK AND SERVICES SECURITY SCHEME.

EXECUTIVE SUMMARY

Proposing Ministry/Body	Ministry of Digital Transformation State Secretariat for Telecommunications and Digital Infrastructure	Date	December 2023
Title of regulation	DRAFT ROYAL DECREE APPROVING THE NATIONAL 5G NETWORK AND SERVICES SECURITY SCHEME		
Report type	Normal ☒ Abbreviated ☐		
SCOPE OF THE PROPOSAL			
Matter regulated	In implementation of the provisions of Royal Decree-Law 7/2022, of 29 March 2022, on requirements to guarantee the security of fifth-generation electronic communications networks and services, in particular, in application of Chapter IV, the proposal approves the National Security Scheme of 5G networks and services [Esquema Nacional de Seguridad de las redes y servicios 5G] (hereinafter, ENS5G), in order to achieve a reliable environment for the development and adoption of 5G networks and services.		
Objectives	- To carry out comprehensive and integral handling of the security of 5G networks and services, considering the contributions within the reach of each agent in the 5G value chain. - To ensure the continued and secure operation of the 5G network and services. - To drive end-to-end security of the ecosystem generated by		

	5G technology. - To strengthen security in the installation and operation of 5G electronic communications networks and in the provision of mobile and wireless communications services supported by 5G networks. - To promote a sufficiently diversified market for suppliers in 5G electronic communications networks and services, in order to ensure security based on technical, strategic and operational reasons and to avoid, for those reasons, the presence of suppliers with a high risk or medium risk rating in certain network elements or areas. - To strengthen the protection of national security. - To bolster industry and promote national R & D & I activities in cybersecurity related to 5G technology.
Main alternatives considered	There is no alternative to the approval of this regulation, since Article 21 of Royal Decree-Law 7/2022, of 29 March 2022, obliges the Government to approve, by Royal Decree, on the proposal of the Ministry of Digital Transformation, following a report of the National Security Council, a National Security Scheme of 5G Networks and Services.
CONTENT, LEGAL ANALYSIS AND DESCRIPTION OF THE PROCESS	
Type of regulation	Royal Decree
Structure of the regulation	The draft consists of an expository part, a single article approving the ENS5G, two additional provisions and four final provisions. The ENS5G to be approved consists of 33 articles divided into eight chapters and three annexes.
Reports to be collected	- CNMC report - Procedure for the provision of information in the field of technical regulations and of rules on Information Society services provided for in Directive (EU) 2015/1535 - Report of the Technical Secretariat-General of the Ministry of

	Digital Processing - Report of the Technical Secretariat-General of the Ministry of Ecological Transition and Demographic Challenge. - Report of the National Security Council - Opinion of the Council of State	
Hearing Proceedings	In accordance with the provisions of Article 26.2 of Law 50/1997, of 27 November 1997, of the Government and Article 133.1 of Law 39/2015, of 1 October 2015, of the Common Administrative Procedure of Public Administrations, between 30 May and 22 June 2022, prior public consultation has been carried out, through the website of the Ministry of Economic Affairs and Digital Transformation. Likewise, the procedure of public hearing must be carried out, in accordance with the provisions of Articles 26.6 of Law 50/1997, of 27 November 1997, and 133.2 of Law 39/2015, of 1 October 2015.	
IMPACT ANALYSIS		
Compliance with the distribution of powers	The Royal Decree and the scheme it approves are issued under the State competences in the field of telecommunications and public security, established in Articles 149.1.21 and 149.1.29 of the Constitution.	
Economic and budgetary impact	Overall economic impact	According to European Commission studies, the estimated benefits of introducing 5G in four productive sectors (automotive, health, transport and utilities) would gradually increase to EUR 62.5 billion per year within the European Union, which would amount to EUR 113 billion by adding the indirect impacts. The same study estimates that Spain would enjoy EUR 14.6 billion in indirect benefits in the four sectors examined as well as major job growth. Confidence in the security of 5G networks and services is key to extending their use

		between citizens and businesses.
	With regard to competition	☐ the regulation does not have significant effects on competition. ☒ the regulation has positive effects on competition. ☒ the regulation has negative effects on competition.
	From the point of view of administrative burdens	☐ It entails a reduction in administrative burdens. ☐ It incorporates new administrative burdens. ☒ It does not affect the administrative burden.
	From the point of view of budgets, the regulation: ☒ Does not affect the budgets of Public Administrations	☐ entails an expense

	☒ Does not affect the budgets of State Administration	☐ entails revenue
Gender impact	The regulation has a gender impact of the following character	Negative ☐ None ☒ Positive ☐
Other impacts considered		-Impact on the fight against depopulation and climate change. -Impact in relation to equal opportunities, non-discrimination and universal accessibility for persons with disabilities. -Impact on childhood adolescence and family.
Other considerations		

A. SCOPE OF THE PROPOSAL

1. MOTIVATION

- **Causes:**

Fifth generation or 5G mobile communications are a new paradigm of electronic communications with major transformation potential for the benefit of society and the economy, as they open up the possibility of incorporating new functionalities that will have a major impact, such as network computing, and make it possible to create virtual networks, offer low latency and provide high added-value services in areas such as medicine, transport and energy.

Both the European Union and Spain are therefore promoting the rapid deployment of 5G networks and the realisation of projects demonstrating their usefulness for different sectors through the provision of 5G services.

5G networks and services have comparative security advantages over previous generations. However, they also present specific risks arising, for example, from their more complex, open and disaggregated network architecture and their ability to transport huge volumes of information and enable the simultaneous interaction of multiple people and things. Their interconnection with other networks and the transnational nature of many of the threats have an impact on their security, and the foreseeable widespread use of these networks for functions essential to the economy and society will increase the potential impact of the security incidents they suffer.

These new specific security risks of 5G mobile communications were addressed in regulation through Royal Decree-Law 7/2022 of 29 March 2022 on requirements to ensure the security of fifth-generation electronic communications networks and services, which fully incorporates the European Commission Recommendation (EU) 2019/534 of 26 March 2019 on the cybersecurity of 5G networks, as well as the recommendations that the European Commission's Communication of 29 January 2020 on the 'Safe Deployment of 5G in the EU – Implementation of the European Commission EU toolbox' (COM/2020/50 final) provided Member States with regard to the use of this 'toolbox'.

The aforementioned Royal Decree-Law 7/2022, of 29 March 2022, provides for its regulatory development through the National System of Security of Networks and 5G Services (ENS5G).

In accordance with Article 5.3 of the aforementioned Royal Decree-Law, the ENS5G will carry out a comprehensive treatment of the security of 5G networks and services, taking into account the contributions within the reach of each agent of the 5G value chain, as well as the regulations, recommendations and technical standards of the European Union, the International Telecommunication Union (ITU) and other international organisations, in order to guarantee the ultimate objective of the safe usage and operation of 5G networks and services in Spain.

For its part, Article 20 of the Royal Decree-Law provides that, in order to ensure the continued and secure operation of the 5G network and services, the ENS5G will carry out a risk analysis at national level on the security of 5G networks and services and identify, specify and develop measures to mitigate and manage the risks analysed.

Finally, in accordance with Article 21 of the Royal Decree-Law, the ENS5G will be approved by the Government, by Royal Decree, on the proposal of the Ministry of Digital Transformation, following a report by the National Security Council.

This regulation approves the ENS5G, developing the provisions of Royal Decree-Law 7/2022, of 29 March 2022, on requirements to guarantee the security of fifth-generation electronic communications networks and services.

- **Affected groups:**

The regulation will apply to:

a) Natural or legal persons operating 5G networks and providers of electronic communications services based wholly or partly on those 5G networks.

   This includes mobile operators holding administrative concessions for the use of radio spectrum and virtual mobile operators, as well as operators using 5G technology to provide communications services. It also includes operators operating private (or corporate) electronic communications networks, which will be more frequent with 5G than it is now with 4G technology.

b) Suppliers of equipment and services for the operation of 5G networks and services, external to operators (collectively designated in the regulation as ‘suppliers’).

   Part of the regulation affects them directly, that is to say, it contains provisions that may be enforced and sanctioned by the competent authorities. It concerns, on the one hand, the obligations of collaboration in the supervisory functions of the Administration, and, on the other, the requirements for the certification of products, processes or services, or of subjecting to audit that the regulation imposes.

However, the regulation furthermore also affects them indirectly, by requiring operators of 5G networks and services to comply with security requirements in relation to their suppliers. This set of regulations includes provisions that may have a significant impact on suppliers. For example: the regulation provides that operators may be required to cease their relationship fully or partially with certain suppliers that are classified as high-risk.

c) Corporate users of 5G networks.

They may be entities that manage a layer or segment of the network for their own purposes (e.g., a hospital for its remote medicine applications). Due to their interfacing with the main network, they can be a gateway to an outside attack.

In addition, in so far as it ensures the security of 5G networks and services, the regulation benefits all users of these networks and services, in particular public administrations, which can use them as a secure and effective channel of communication with citizens.

- **Public interest issues**

The public interest concerned is to ensure maximum protection of communications networks and services based on 5G technology and networks against security attacks or incidents, as a means of building trust in the new 5G services.

The foreseeable widespread use of these networks in functions essential to the economy and society, and the dependence on external suppliers, means that at a time of serious geopolitical tensions, the cybersecurity of 5G networks becomes a national security priority.

In addition, there are fundamental rights involved, such as the right to personal and family privacy or to the secrecy of communications, guaranteed at the highest regulatory level by the Spanish Constitution.

In the long term, the reinforcement of the European Union’s technological autonomy is also involved.

Additionally, given the potential of this technology for the growth of different economic sectors, the economic and social growth of Spain and the well-being of citizens who access essential services or exercise their right to information through 5G networks, are also affected.

- **Why this is the appropriate time to do so:**

Operators should adapt their cybersecurity policies as soon as possible to the measures set out in the regulation, so that fifth-generation mobile communications networks and services are secure from the outset.

In addition, it should be borne in mind that the second paragraph of the third final provision of Royal Decree-Law 7/2022, of 29 March 2022, established a period of six months from its entry into force for the approval of the ENS5G, which has already been exceeded.

2. Objectives.

The purpose of the regulation is to ensure the reliability of 5G networks and services, and thereby the development of value-added services for the economy and society, in areas as diverse as transport, healthcare, industry, agriculture, logistics, energy or the media.

To this end, specific objectives are set:

- To carry out comprehensive and integral handling of the security of 5G networks and services, considering the contributions within the reach of each agent in the 5G value chain.
- To ensure the continued and secure operation of the 5G network and services.
- To drive end-to-end security of the ecosystem generated by 5G technology.
- To strengthen security in the installation and operation of 5G electronic communications networks and in the provision of mobile and wireless communications services supported by 5G networks.
- To promote a sufficiently diversified market for suppliers in 5G electronic communications networks and services, in order to ensure security based on technical, strategic and operational reasons and to avoid, for those reasons, the presence of suppliers with a high risk or medium risk rating in certain network elements or areas.
- To strengthen the protection of national security.
- To bolster industry and promote national R & D & I activities in cybersecurity related to 5G technology.

3. Alternatives.

There is no alternative to the approval of this regulation, since Article 21 of Royal Decree-Law 7/2022, of 29 March 2022, obliges the Government to approve, by Royal Decree, on the

proposal of the Ministry of Digital Transformation, following a report of the National Security Council, a National System of Security of 5G networks and services.

4. Adherence to the principles of sound regulation.

The regulation complies with the principles of good regulation set out in Article 129 of Law 39/2015 of 1 October 2015 on the common administrative procedure of public administrations.

The principle of necessity is fulfilled, since this Royal Decree is issued by Royal Decree-Law 7/2022, of 29 March 2022, to guarantee a goal of general interest, such as security and trust in electronic communications.

it complies with the principle of proportionality as the measures are appropriate to the risks identified in each case;

The regulation complies with the principle of legal certainty as soon as it implements the provisions of Royal Decree-Law 7/2022, of 29 March 2022, on requirements to guarantee the security of fifth-generation electronic communications networks and services, and completes the current regulatory framework on security, adding requirements and controls only when the uniqueness of 5G networks and services and their risks, so require.

The principle of transparency is respected, as stakeholders have been able to participate in the procedure for drawing up the regulation and will be published.

Finally, the principle of efficiency is fulfilled, since administrative burdens have been limited to the minimum necessary to achieve the aim of ensuring the security of 5G networks and services.

5. Annual Legislative Plan

Royal Decree-Law 7/2022, of 29 March 2022, corresponds to the preliminary draft law on requirements to ensure the security of fifth-generation electronic communications networks and services, provided for in the Annual Legislative Plan of the General State Administration for 2022, approved by agreement of the Council of Ministers of 11 January 2022.

This draft, which implements this Royal Decree-Law, is not, however, foreseen in the Annual Legislative Plan for 2023.

B. CONTENT, LEGAL ANALYSIS AND DESCRIPTION OF THE PROCEDURE

1. Content.

The regulation consists of an expository part, a single article approving the ENS5G, two additional provisions and four final provisions.

The ENS5G to be approved consists of 33 articles divided into eight chapters and three annexes.

The explanatory memorandum explains the reasons behind the adoption of the regulation and the articles of the Royal Decree-Law that are being implemented.

The single article approves the National Security Scheme of 5G Networks and Services.

The first additional provision states that the Government, by Royal Decree, on the proposal of the Ministry of Digital Transformation, following a report of the National Security Council, will review the National Network Security Scheme of 5G Networks and Services when circumstances give rise to this and, in any event, every four years.

The second additional provision states that Royal Decree-Law 7/2022 of 29 March 2022 and ENS5G will apply to generations of electronic communications after the fifth generation, as long as there is no specific regulation for them.

The first final provision on the title of competence states that the Royal Decree and the scheme it approves are issued under the provisions of Article 149.1.21 and Article 149.1.29 of the Constitution, which confer on the State, exclusive competence in matters of general telecommunications regime and in matters of public security, respectively.

The second final provision declares that General Law 11/2022, of 28 June 2022, on Telecommunications, and its implementing regulations, to be of supplemental application, and states that in all matters not regulated in said legislation, the Royal Decree-Law 12/2018, of 7 September 2018, on the security of networks and information systems and Law 8/2011, of 28 April 2011, establishing measures for the protection of critical infrastructures, as well as its respective development regulations, will be of supplemental application.

The third final provision on regulatory development enables the holder of the Ministry of Digital Transformation to implement the provisions of this Royal Decree and the scheme it approves, and to modify by order the contents of the annexes according to the evolution of technological progress, the approval of new technical standards and certification schemes of telecommunication equipment and connected products and the development of different configurations and technical parameters of 5G networks and services and future generations of electronic communications.

The fourth final provision provides that the regulation will enter into force on the day following its publication in the Official State Gazette.

As regards the content of ENS5G, which is approved:

Article 1 states that the regulation is issued in implementation of Royal Decree-Law 7/2022 of 29 March 2022, in particular, in application of Chapter IV thereof.

Article 2 refers to the objectives of the regulation, which have already been analysed.

Article 3 states that the definitions laid down in Royal Decree-Law 7/2022 of 29 March 2022, General Law 11/2022 of 28 June 2022, on Telecommunications, and the European Electronic Communications Code will be used.

Article 4 provides that the regulation will apply to 5G operators, 5G suppliers and 5G corporate users who have rights of use in the public radio domain to install, deploy or operate a 5G private network or to provide 5G services for professional or self-providing purposes.

Article 5 identifies the elements, infrastructures and minimum resources that make up a 5G electronic communications network, referring its detailed description to Annex I. It also sets out the critical elements of a 5G network, which must be located, as a general regulation, in national territory (collecting possible exceptions).

Article 6 refers to the comprehensive treatment of security in accordance with international Community and national legislation approved or that may be approved, requiring the obliged parties to carry out, by means of a holistic method, an analysis of the vulnerabilities, threats and risks affecting them as economic agents and of the various components, as well as an adequate and comprehensive management of those risks through the use of techniques and measures appropriate for achieving their mitigation or elimination, and to achieve the ultimate objective of the safe operation and operation of 5G networks and services.

Article 7 stresses that risk analysis and management is an essential part of the security process, and should be an ongoing and constantly updated activity.

Article 8 refers to ongoing monitoring and periodic reassessment.

Article 9 states that the risk analysis at national level is the one set out in Annex II and has been carried out taking into account various elements such as information collected from obliged parties, the examination of vulnerabilities linked to the supply chain of 5G networks and services, the assessment of the degree of dependence of suppliers, the risk of interruption of supply due to economic, corporate or commercial circumstances affecting suppliers or the assessment of the effectiveness of the security measures applied.

Article 10, on risk management at national level, states that the criteria, requirements, conditions and deadlines for obliged parties to design and implement risk mitigation techniques and measures are those set out in Annex III.

Article 11 implements the provisions of Article 14 of Royal Decree-Law 7/2022 of 29 March 2022 in relation to the procedure and aspects to be assessed by the Council of Ministers for the classification of suppliers as high risk, and the elements to be taken into account when ordering the possible replacement of the equipment, products and services provided by those suppliers. Likewise, in accordance with the provisions of the aforementioned Royal Decree-Law, it is stated that high-risk suppliers whose telecommunication equipment, hardware, software or ancillary services provided are used solely and exclusively in 5G private networks, or for the provision of 5G services under self-provision, are classified as medium-risk suppliers.

Article 12, on the determination of locations where equipment of qualified high-risk suppliers may not be installed, states that the National Security Council, following a report by the Ministry of Digital Transformation, may determine the locations, areas and centres in which equipment of qualified high-risk suppliers may not be installed. For the installation, modification or adaptation of radio stations that provide coverage to these locations, areas and centres, 5G operators must request authorisation from the Ministry of Digital Transformation.

Article 13 obliges 5G operators to design a strategy for diversification in the supply chain and to have in the access network, transmission equipment that is provided by at least two different suppliers. It also provides criteria to be taken into account by the Council of Ministers, in order to decide whether it is possible to maintain a single supplier if the number of suppliers is reduced as a result of business concentrations. It also points to the assumptions and procedure by which the Ministry of Digital Transformation is able to modify the strategy of diversification in the supply chain of a 5G operator.

Article 14 focuses on the risk analysis to be carried out by 5G operators in relation to all the elements, infrastructures and resources of the network listed in Annex I; the factors to be taken into account are listed, operators are obliged to seek from their suppliers the security practices and measures adopted in the products and services they have supplied to them and to include a prioritisation and hierarchy of risks according to certain parameters that are also listed. By 1 October 2024, 5G operators must submit a risk analysis, and then every two years thereafter.

Article 15, on risk analysis by 5G suppliers, requires the analysis of the risks of telecommunications equipment, hardware and software and ancillary services involved in the functioning or operation of 5G networks or in the provision of 5G services, and to provide such analysis to the Ministry when required. In the case of suppliers classified as high risk or

medium risk, the analysis is to be submitted within six months of that rating and every two years thereafter.

Article 16, on risk analysis by 5G corporate users, obliges providing this risk analysis to the Ministry of Digital Transformation, when such users are required to do so.

Article 17 allows the Ministry of Digital Transformation to collect from the obliged parties the information necessary for the risk analysis, and qualifies as a serious infringement the failure to provide such information within 15 working days. The information is considered confidential, and may not be used for a purpose other than the fulfilment of the objectives and obligations established in Royal Decree-Law 7/2022, of 29 March 2022, in the ENS5G, and in the acts that are issued in execution of both provisions.

Article 18 proclaims the general duty of all obliged parties to manage security risks.

Article 19 focuses on security management by 5G operators, listing obligations for all operators (such as to adopt contingency plans and measures, comply with European standards or specifications and certification schemes, undergo, at their cost, a safety audit or require their suppliers to comply with safety standards) and additional ones for those operators who own or operate critical elements of a 5G public network (such as prohibitions on the use of equipment by high-risk suppliers in critical network elements or in certain locations, areas and centres). 5G operators must submit to the Ministry of Digital Transformation a description of the technical and organisational measures designed and implemented to manage and mitigate risks before 1 October 2024 and every two years thereafter. In addition, 5G operators that own or operate critical elements of a 5G public network must submit to the Ministry of Digital Transformation a strategy of diversification in the supply chain before 1 October 2024 and thereafter each time it is subject to modification. Information on the state of implementation of this strategy must be submitted by 1 October of each year.

Article 20, on security management by 5G suppliers, contains a list of obligations that includes carrying out a security audit of their equipment, products and services, providing information on possible interferences by third parties in the design, operation and function of their equipment, products and services, or collaborating with 5G operators and 5G corporate users by providing information and certifying compliance with standards and certifications. 5G suppliers should prepare a report on technical and organisational measures designed and implemented to manage and mitigate risks and provide such a report to the Ministry when required. In the case of suppliers classified as high risk or medium risk, the report shall be submitted within six months of that rating, and every two years thereafter.

Article 21, on security management by 5G corporate users, states that they may not use in the critical network elements telecommunication equipment transmission systems, switching or routing equipment and other resources that allow the transport of signals, hardware, software or ancillary services of suppliers that have been classified as medium risk, and that they must

provide to the Ministry of Digital Transformation, where required, a description of the technical and organisational measures designed and applied to manage and mitigate risks.

Article 22, on security management by public administrations, states that for reasons of national security, in the installation, deployment and operation of 5G networks, whether public or private, or the provision of 5G services, publicly available or self-provided, PAs may not use equipment, products and services provided by high-risk or medium-risk suppliers.

Article 23 states that, in compliance with the obligations laid down in the previous articles, the obliged parties shall take into account and apply the provisions of Royal Decree-Law 7/2022, of 29 March 2022, in the ENS5G and in the acts that are issued in implementation of both provisions.

Article 24 allows the Ministry of Digital Transformation to collect from the obliged parties the information necessary for risk management and qualifies as a serious infringement the failure to provide such information within 15 working days. The information is considered confidential, and may not be used for a purpose other than the fulfilment of the objectives and obligations established in Royal Decree-Law 7/2022, of 29 March 2022, in the ENS5G, and in the acts that are issued in execution of both provisions.

Article 25 states that all obliged parties, as well as public administrations, manufacturers, importers, distributors and those who place on the market and commercialise terminal equipment and devices to connect to a 5G network and to be able to provide 5G services, must cooperate and send the information required for the modification and execution of the ENS5G.

Article 26 states that, by order of the person responsible at the Ministry of Digital Transformation, the use of a specific equipment, system, programme or service may be made subject to prior certification under Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on cybersecurity, or certification schemes and technical standards for the certification of 5G equipment and products that can be approved at European or international level.

Article 27 states that the regulation applies without prejudice to foreign investment and competition rules.

Article 28, on terminal equipment, provides that the manufacture, import, distribution, placing on the market and placing on the market of terminal equipment and devices to connect to a 5G network and to be able to provide 5G services will be conditional on compliance with the security requirements for digital products and the applicable essential requirements related to cybersecurity, adopted in accordance with European legislation, in particular in relation to the protection of personal data, privacy, and protection against fraud.

Article 29 concerns the international cooperation to be developed by the Ministry of Digital Transformation, in particular at the level of the European Union

Article 30 refers to the competence of the Ministry of Digital Transformation for the implementation of ENS5G, and should coordinate with the other bodies responsible for cybersecurity and critical infrastructure to ensure a consistent implementation of ENS5G.

Article 31 breaks down the powers for the implementation of the ENS5G that correspond to the Ministry of Digital Transformation, among which are, for example, the development, specification and detail of the content of the ENS5G, the carrying out of audits to verify and monitor compliance with the obligations imposed or the granting of public aid.

Article 32 assigns the Ministry of Digital Transformation all the powers of the inspection function.

Article 33, on the penalty regime, refers to the provisions of Articles 30 and 31 of Royal Decree-Law 7/2022 of 29 March 2022.

Annex I describes the elements, infrastructures and resources that make up a 5G network.

Annex II contains the risk analysis at national level.

Annex III sets out risk management at national level.

2. Legal analysis.

- **Relationship with other national regulations**.

- The regulation implements Royal Decree-Law 7/2022, of 29 March 2022, on requirements to guarantee the security of fifth-generation electronic communications networks and services, and in particular Chapter IV thereof, relating to ESN5G.

- Law 9/2014 of 9 May 2014 (particularly Article 44) contains generic security obligations that 5G network operators still have to comply with.

- Royal Decree-Law 12/2018 of 7 September 2018 on the security of networks and information systems establishes requirements that operators that have been designated as critical operators under Law 8/2011 of 28 April 2011 establishing measures for the protection of critical infrastructures must continue to comply.

- Order IET/1090/2014, of 16 June 2014, regulating the conditions relating to the quality of service in the provision of electronic communications services regulates, in Chapter VI, the mandatory notification to the Authorities of cases of interruption of telephone service and

Internet access and its Chapter VII, refers to the inspector power of the State Secretariat for Telecommunications and Digital Infrastructures.

- The National Cybersecurity Plan approved on 29 March 2022 by the Council of Ministers specifies, through specific actions and projects, different measures included in the National Cybersecurity Strategy 2019.

- The regulation is also consistent with Component 15 of Spain's Recovery, Transformation and Resilience Plan, which aims to ensure connectivity throughout the national territory, lead the deployment of networks and services based on 5G technologies in Europe, and position Spain as an international hub of cybersecurity infrastructures and talent. This component is formulated through two fundamental plans of the Digital Agenda of the Government of Spain (Spain Digital 2025): the Plan for Connectivity and Digital Infrastructures, and the 5G Technology Boost Strategy.

- **Consistency with European Union law**

- The European Electronic Communications Code, established by Directive 2018/1972 of 11 December 2018, requires that measures be taken to safeguard the security of networks and services. and to prevent or minimise the impact of security incidents.

- 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) and Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), are also related to this regulation, as the strengthening of security in 5G networks will result in greater protection against illegitimate interference in the rights to privacy and the secrecy of communications in this area.

- The regulation is also consistent with the Directive on the Security of Networks and Information Systems (NIS), adopted in 2016, which established security obligations for operators of essential services (in vital sectors such as energy, transport, health and finance) and digital service providers (online markets, search engines and cloud services) and with its 2022 revision (NIS Directive2).

- This project implements Commission Recommendation (EU) 2019/534 of 26 March 2019, Cybersecurity of 5G networks, which proposed coordinated action by Member States to analyse the security risks of 5G technology and the collection and implementation of good

practices to ensure the security of these networks. Member States supported this Recommendation in the conclusions agreed by the Council of the European Union of 3 December 2019.

- As a result of the Recommendation referred to in the previous paragraph, the European Toolbox was published on 29 January 2020. On the same day, the European Commission issued the Communication 'Secure 5G deployment in the EU – Implementation of the EU Toolbox' which states that the conclusions and actions recommended in the Toolbox must be 'key measures' to be implemented by the Member States and the European Commission to ensure the security of these networks in Europe.

- The regulation is also consistent with Regulation EU 2019/881 of the European Parliament and of the Council of 17 April 2019 on cybersecurity, which regulates the procedure under which European information and communication technology cybersecurity certification schemes can be adapted.

- Lastly. the regulation relates to the proposal for a Cyber Resilience Regulation, which aims to establish mandatory cybersecurity requirements for products consisting of computer equipment (hardware) and software with connected digital elements.

- **Regulations that are amended or repealed**

No regulations are amended or repealed.

- **Entry into force**

According to its fourth final provision, the Royal Decree will enter into force on the day following that of its publication in the 'Official State Gazette'.

In accordance with the provisions of Article 23 of Law 50/1997 of 27 November 1997 of the Government, this is justified by the need to establish as soon as possible the rules applicable to the 5G deployments already carried out by operators, avoiding possible security incidents.

In addition, it should be borne in mind that the second paragraph of the third final provision of Royal Decree-Law 7/2022 of 29 March 2022 established a period of six months from its entry into force, for the approval of the ENS5G, which has already been exceeded.

3. Description of the process

- **Public participation**

In accordance with the provisions of Article 26.2 of Law 50/1997, of 27 November 1997, of the Government and Article 133.1 of Law 39/2015, of 1 October 2015, of the Common Administrative Procedure of Public Administrations, in order to publicise the opinion of operators, citizens and any interested party on the elaboration of a new regulation on the National Network Security Scheme 5G Networks and Services between 30 May and 22 June 2022, prior public consultation has been carried out, through the electronic office of the Ministry of Economic Affairs and Digital Transformation.

In the aforementioned consultation, 15 contributions have been received, which have been taken into account when preparing the proposal for a regulation.

In particular, 14 contributions have been received from entities and 1 from an individual:

- AMETIC (20/06/22)
- SPANISH ASSOCIATION FOR STANDARDISATION, UNE (20/06/22)
- CHAMBER OF COMMERCE OF SPAIN (20/06/22)
- CEOE (20/06/22)
- DIGITALES (20/06/22)
- ERICSSON (20/06/22)
- HUAWEI TECHNOLOGIES ESPAÑA, S.L. (20/06/22)
- MASMOVIL IBERCOM, S.A.U. (20/06/22)
- NOKIA ESPAÑA (20/06/22)
- ORANGE ESPAGNE, S.A.U. (20/06/22) (CONFIDENCIAL)
- SAMSUNG ELECTRONICS IBERIA, S.A.U. (19/06/22)
- TELEFÓNICA ESPAÑA (20/06/22) (CONFIDENCIAL)
- VODAFONE ESPAÑA, S.A.U. AND VODAFONE ONO, S.A.U. (20/06/22)
- ZTE ESPAÑA, S.L.U. (20/06/22)
- MIGUEL BAÑÓN (16/06/22)

Likewise, the procedure of public hearing must be carried out, in accordance with the provisions of Articles 26.6 of Law 50/1997, of 27 November 1997, and 133.2 of Law 39/2015, of 1 October 2015.

- **Reports to be collected**

-

- CNMC report

- Procedure for the provision of information in the field of technical regulations and of rules on Information Society services provided for in Directive (EU) 2015/1535

- Report of the Technical Secretariat-General of the Ministry of Digital Processing

- Report of the Technical Secretariat-General of the Ministry for Ecological Transition and the Demographic Challenge.

- Report of the National Security Council

- Opinion of the Council of State.

C. COMPLIANCE WITH THE DISTRIBUTION OF POWERS

The regulation is in line with the constitutional order of distribution of competences, being issued by virtue of the exclusive competences in telecommunications and public security conferred on the State by Articles 149.1.21 and 149.1.29 of the Spanish Constitution (EC).

With regard to the exclusive competences of the State in the field of telecommunications and the general system of communications of **Article 149.1.21** EC, the first of them is connected with the technical aspects of the emission relating to the use of radio or electromagnetic waves (public radio domain), which justifies a 'joint ordering of all telecommunication and radio communication variants' [STC 78/2017, of 22 June, FJ 4 a), citing STC 168/1993 of 27 May, FJ 4]. For its part, the exclusive competence of the State in respect of the 'general communications regime' 'includes, of course, all the regulatory powers over it (SSTC 84/1982, FJ 4, and 38/1983, FJ 3); but it also implies a plus', since it 'may entail the attribution of the implementing powers necessary to set up a materially unitary system (STC 195/1996, 28 November, FJ 6)'. Therefore, it falls within the competence of Article 149.1.21 of the EC to regulate electronic communications services provided by any technology and therefore also to guarantee the availability and 'security' of networks or services, a term defined in the European Electronic Communications Code, as 'the ability of electronic communications networks and services to resist, with a certain level of trust, any action that

compromises the availability, authenticity, integrity and confidentiality of such networks and services, of data stored, processed or transmitted, and the security of the related services that those electronic communications networks and services offer or make accessible'.

As STC 8/2016 of 21 January 2016, FJ 3, recalls: 'From a latest, more global perspective, it also integrates in the field of telecommunications and general communications systems (and therefore the State has exclusive competence under 149.1.21 EC) the formation, regulation or configuration of the telecommunications sector itself (electronic communications) taking into account technological convergence (and services) and the regulatory framework of electronic communications of the European Union to ensure homogeneous regulation throughout Spain. This homogeneity is necessary, not only for the development and innovation of the sector, but also for the guarantee of citizens' rights in the framework of the information society (or knowledge society), given that the development of communications and new information technologies is an essential factor in achieving the social, economic and territorial cohesion necessary to avoid, or at least reduce, the so-called digital divide'.

In relation to the title of competence on public security of **Article 149.1.23** we refer to the provisions of the JTF of Judgment 142/2018 of 20 December 2018, which have just been transcribed, as well as to the previous paragraphs in relation to the foreseeable widespread use of these networks in essential functions for the economy and society, taking into account that dependence on external suppliers, requires that at a time such as the present with serious geopolitical tensions, the cybersecurity of 5G networks becomes a priority national security objective, within which public security is framed.

This is stated in the judgment of the Constitutional Court 84/2016 of 3 November 2016, stating that 'it can be said that there is a substantial coincidence between the meaning and purpose of the titles of competence in matters 4 and 29 of Article 149.1. EC and the concept of national security, defined in Article 3 of Law 36/2015, as: the action of the State aimed at protecting the freedom, rights and welfare of citizens, to guarantee the defence of Spain and its constitutional principles and values, as well as to contribute together with our partners and allies to international security in the fulfilment of the commitments made.

Finally, it should be noted that the Autonomous Communities and Local Entities have had the opportunity to decide on the draft regulation in the public consultation procedure carried out between 30 May and 20 June 2022 without any of them submitting contributions. They may likewise participate in the corresponding public hearing procedure.

D. ECONOMIC AND BUDGETARY IMPACT.

1. Overall economic impact.

Electronic communications has been a markedly dynamic and innovative sector, generally linked to investment in new network deployment.

At present there is an opportunity to continue with this innovative dynamic, through investment in 5G networks, but this will only be possible if appropriate measures are introduced to ensure the integrity, continuity and security of these networks, avoiding the risks that their widespread deployment could lead to.

In addition, due to its cross-cutting nature, the telecommunications sector not only ensures the provision of increasingly essential services, such as teleworking, telemedicine and online learning, it also promotes the growth of other sectors, like the content industry, big data, the Internet of Things and connected car services. This enables smart management of transport and energy resources and helps bridge the digital divide between different regions.

In this sense, the new 5G networks are positioned as a key element in accelerating the digital transformation of society and the economy.

In our more immediate environment, analyses from the European Commission predict that the direct annual economic impact of the projected benefits of introducing 5G in four productive sectors (automotive, health, transport and utilities) within the EU would gradually increase to EUR 62.5 billion by 2025, and to EUR 113 billion counting the indirect impact. The same study estimates that Spain would enjoy EUR 14.6 billion in indirect benefits in the four sectors examined as well as major job growth.

In conclusion, it should be noted that in these current times of international uncertainty, telecommunications is one of the most dynamic sectors of the economy and, thanks to its cross-cutting nature, is amongst those with the greatest potential to contribute to growth, productivity and employment, and thus also to economic development and social welfare.

The security measures proposed in the draft are also expected to have a neutral impact on prices, as operators and service providers are already making strong investments to provide connectivity through 5G, with security being a marginal aspect of these costs.

In any case, the economic effort devoted to security measures should be regarded as an investment, since it reduces the cost of replacement of the service and possible compensation, and also increases the revenue from the entry of new customers relying on the new technology.

Because of its cross-sectoral impact, the introduction of 5G technology is bound to create an important positive effect on employment in many sectors.

Although moreover, compliance with the specific security measures provided for in this regulation will also have a positive effect on job creation in sectors such as R & D & I, certification or auditing, with the specific objective of the regulation being to strengthen industry and promote national R & D & I in cybersecurity.

The effect of the regulation on consumers is also expected to be positive, as the increased choice between technologies resulting from the introduction of 5G itself adds the intangible benefits associated with increased security and confidence in the use of the new technology.

2. Effects on competition and market unity

The regulation has positive effects as provisions related to the diversification of suppliers in the supply chain and measures aimed at strengthening industry and promoting national R & D & I in cybersecurity can contribute to the emergence and growth of new players.

On the other hand, the restrictions on free competition resulting from the restriction of the participation of high-risk or medium-risk suppliers safeguard national security by ensuring the continuity of essential services and applications that rely on these networks (health, civil protection, education, etc.) and are only essential, in the light of a rigorous risk analysis and decisions taken by other Member States or by the EU itself.

Therefore, given that the regulation is expected to have both positive and negative effects on competition, both are expected to be counteracted, creating a new competitive situation in which new suppliers contribute to the technological autonomy of the European Union, avoiding the risks arising from cyberattacks.

3. Budgetary impact.

- **From a revenue point of view:**

The draft will not involve the generation or forecasting of revenue for the State Treasury or for the Treasury of other public administrations.

- **From an expenditure point of view:**

The draft will not involve the realisation of expenses from the General State Budgets, nor will it involve the assumption of costs or expenses for the State Treasury or for the Treasury of other Public Administrations.

The coordination, inspection and sanction tasks entrusted to the Ministry of Digital Transformation will be carried out with the means and resources already assigned to this Ministry.

E. DETECTION AND MEASUREMENT OF ADMINISTRATIVE BURDENS.

No new burdens are imposed, since the administrative burdens for operators, suppliers and corporate users were already provided for in Royal Decree Law 7/2022, of 29 March 2022, on requirements to guarantee the security of fifth-generation electronic communications networks and services, which is now being developed, so we must refer to the measurement of burdens contained in the MAIN of this regulation.

F. GENDER IMPACT

The draft does not have any impact on gender, as its content does not contain measures of any kind that could affect the equality of opportunities for women and men.

G. IMPACT ON THE FIGHT AGAINST DEPOPULATION AND CLIMATE CHANGE

The security of 5G technology is a key element for the territorial structuring of the country, since secure access to the new networks and to the new digital content and services that can be provided through them are an essential element for the incorporation of citizens and businesses into the Information and Knowledge Society, thereby promoting social cohesion and economic development and contributing to the development of the new eGovernment.

In this sense, the measures introduced by the regulation become important pillars to achieve the elimination of the digital divide and to structure different territories so that access to new services and applications such as telemedicine, online learning or teleworking can be guaranteed anywhere in Spain, favouring the settlement and fixing of population in rural areas.

In addition to this, telecommunications is a key factor in combating climate change. This includes the European Union target of reducing greenhouse gas emissions by 55 %, compared with 1990 levels, by 2030.

The Information and Communication Technology sector generates relatively few emissions, while at the same time it can play a critical role in combating climate change by facilitating more efficient use of energy resources in other sectors.

In this sense, the energy savings of the networks themselves should be highlighted, thanks to the increased energy efficiency of 5G technologies, as well as the transformational role that

the ICT sector as a whole has played in the innovation and redesign of business models of all sectors in the so-called digital era, making it the catalyst that other sectors need to contribute to the new low greenhouse gas emissions economy, facilitating innovative uses of 'smart' products and services, helping to generate environmental benefits and allowing energy cost savings to users.

In addition, telecommunications are very useful in environmental and climate monitoring, including weather forecasting, and critical for early warning and disaster mitigation communications.

The conclusions of the study "Telecommunications and CO2: The Role of Mobile Technology against Climate Change," indicate that 13 mobile technology initiatives can reduce CO2 emissions by 113 million tonnes (equivalent to emissions from around 50 million vehicles) and generate energy savings of EUR 43 billion in Europe.

This will require 1.04 billion new mobile connections, 87% of which would be machine-to-machine (M2M).

Its application in Spain would entail a reduction of 10.6 million tonnes of CO2 emissions (equivalent to the emissions generated by 4.7 million vehicles, which is 15 % of the current fleet), and energy savings of EUR 4.042 billion. In the case of Spain, this will require 98 million new connections, 85 million of which would be M2M.

Energy savings will mainly come from greater use of smart M2M services (smart electricity grids, smart logistics, smart cities and smart production systems) as well as the replacement of physical activities with virtual ones.

This virtualisation process would replace processes, movements, meetings and travel with low-emission virtual alternatives. Some examples here would be reducing travel by using virtual meeting rooms with telecommunications connectivity, promoting the use of telecommunications products so employees can work remotely from home, and using mobile communications to improve e-commerce processes and to facilitate ordering and shipping systems for purchases. These initiatives would not only allow us to adapt to possible health containment measures for possible epidemics, but at the same time would reduce CO2 emissions in Europe by more than 22 million tonnes, as well as potential savings in energy consumption of EUR 14.1 billion (in Spain: savings of 2 million tonnes of CO2 emissions and EUR 1.33 billion).

H. OTHER IMPACTS

The draft act has no impact on equal opportunities, non-discrimination or universal accessibility for persons with disabilities.

There are also no significant impacts of the draft regulation in relation to childhood, adolescence or family.