



European Commission recommends common EU approach to the security of 5G networks

Strasbourg, 26 March 2019

Today the European Commission has recommended a set of operational steps and measures to ensure a high level of cybersecurity of 5G networks across the EU.

Fifth generation (5G) networks will form the future backbone of our societies and economies, connecting billions of objects and systems, including in critical sectors such as energy, transport, banking, and health, as well as industrial control systems carrying sensitive information and supporting safety systems. Democratic processes, such as elections, increasingly rely on digital infrastructures and 5G networks, highlighting the need to address any vulnerabilities and making the Commission's recommendations all the more pertinent ahead of the European Parliament elections in May.

Following the support from Heads of State or Government [expressed](#) at the European Council on 22 March for a concerted approach to the security of 5G networks, the European Commission is today recommending a set of concrete actions to assess cybersecurity risks of 5G networks and to strengthen preventive measures. The recommendations are a combination of legislative and policy instruments meant to protect our economies, societies and democratic systems. With worldwide 5G revenues estimated at €225 billion in 2025, 5G is a key asset for Europe to compete in the global market and its cybersecurity is crucial for ensuring the strategic autonomy of the Union.

Vice-President Andrus **Ansip**, in charge of the Digital Single Market, said: *"5G technology will transform our economy and society and open massive opportunities for people and businesses. But we cannot accept this happening without full security built in. It is therefore essential that 5G infrastructures in the EU are resilient and fully secure from technical or legal backdoors."*

Commissioner Julian **King**, in charge of the Security Union, stated: *"The resilience of our digital infrastructure is critical to government, business, the security of our personal data and the functioning of our democratic institutions. We need to develop a European approach to protecting the integrity of 5G, which is going to be the digital plumbing of our interconnected lives."*

Commissioner Mariya **Gabriel**, in charge of the Digital Economy and Society, added: *"Protecting 5G networks aims at protecting the infrastructure that will support vital societal and economic functions – such as energy, transport, banking, and health, as well as the much more automated factories of the future. It also means protecting our democratic processes, such as elections, against interference and the spread of disinformation."*

Any vulnerability in 5G networks or a cyber-attack targeting the future networks in one Member State would affect the Union as a whole. This is why concerted measures taken both at national and European levels must ensure a high level of cybersecurity.

Today's Recommendation sets out a series of **operational measures**:

1. At national level

Each Member State should complete a national risk assessment of 5G network infrastructures by the end of June 2019. On this basis, Member States should update existing security requirements for network providers and include conditions for ensuring the security of public networks, especially when granting rights of use for radio frequencies in 5G bands. These measures should include reinforced obligations on suppliers and operators to ensure the security of the networks. The national risk assessments and measures should consider various risk factors, such as technical risks and risks linked to the behaviour of suppliers or operators, including those from third countries. National risk assessments will be a central element towards building a coordinated EU risk assessment.

EU Member States have the right to exclude companies from their markets for national security reasons, if they do not comply with the country's standards and legal framework.

2. At EU level

Member States should exchange information with each other and with the support of the Commission and the European Agency for Cybersecurity (ENISA), will complete a coordinated risk assessment by 1 October 2019. On that basis, Member States will agree on a set of mitigating measures that can be

used at national level. These can include certification requirements, tests, controls, as well as the identification of products or suppliers that are considered potentially non-secure. This work will be done by the Cooperation Group of competent authorities, as set out under the [Directive on Security of Network and Information Systems](#), with the help of the Commission and ENISA. This coordinated work should support Member States' actions at national level and provide guidance to the Commission for possible further steps at EU level. In addition, Member States should develop specific security requirements that could apply in the context of public procurement related to 5G networks, including mandatory requirements to implement cybersecurity certification schemes.

Today's Recommendation will make use of the **wide-range of instruments** already in place or agreed to reinforce cooperation against cyber-attacks and enable the EU to act collectively in protecting its economy and society, including the first EU-wide legislation on cybersecurity (Directive on Security of Network and Information Systems), the [Cybersecurity Act](#) recently approved by the European Parliament, and the new [telecoms rules](#). The Recommendation will help Member States to implement these new instruments in a coherent manner when it comes to 5G security.

In the field of cybersecurity, the future European cybersecurity certification framework for digital products, processes and services foreseen in the Cybersecurity Act should provide an essential supporting tool to promote consistent levels of security. When implementing it, Member States should also immediately and actively engage with all other involved stakeholders in the development of dedicated EU-wide certification schemes related to 5G. Once they become available, Member States should make certification in this area mandatory through national technical regulations.

In the field of telecoms, Member States have to ensure that the integrity and security of public communications networks are maintained, with obligations to ensure that operators take technical and organisational measures to appropriately manage the risks posed to security of networks and services.

Next steps

- Member States should complete their national risk assessments by **30 June 2019** and update necessary security measures. The national risk assessment should be transmitted to the Commission and European Agency for Cybersecurity by **15 July 2019**.
- In parallel, Member States and the Commission will start coordination work within the NIS Cooperation Group. ENISA will complete a 5G threat landscape that will support Member States in the delivery by **1 October 2019** of the EU-wide risk assessment.
- By **31 December 2019**, the NIS Cooperation Group should agree on mitigating measures to address the cybersecurity risks identified at national and EU levels.
- Once the Cybersecurity Act, recently approved by the European Parliament, enters into force in the coming weeks, the Commission and ENISA will set up the EU-wide certification framework. Member States are encouraged to cooperate with the Commission and ENISA to prioritise a certification scheme covering 5G networks and equipment.
- By **1 October 2020**, Member States – in cooperation with the Commission – should assess the effects of the Recommendation in order to determine whether there is a need for further action. This assessment should take into account the outcome of the coordinated European risk assessment and of the effectiveness of the toolbox.

Background

In its [conclusions](#) of 22 March, the European Council expressed its support for the European Commission recommending a concerted approach to the security of 5G networks. The European Parliament's [Resolution](#) on security threats connected with the rising Chinese technological presence in the Union, voted on 12 March, also calls on the Commission and Member States to take action at Union level.

In addition, the cybersecurity of 5G networks is key for ensuring the strategic autonomy of the Union, as underlined in the Joint Communication "[EU-China, a Strategic Outlook](#)". That is why it is essential and urgent to review and strengthen existing security rules in this area to ensure that they reflect the strategic importance of 5G networks, as well as the evolution of the threats, including the growing number and sophistication of cyber-attacks. 5G is a key asset for Europe to compete in the global market. Worldwide 5G revenues should reach the equivalent of €225 billion in 2025. Another [source](#) indicates that the benefits of the introduction of 5G across four key industrial sectors, namely automotive, health, transport and energy, may reach €114 billion per year.

For More Information

[Recommendation on Cybersecurity of 5G Networks](#)

[Questions and Answers](#)

[Security Union: 15 out of 22 legislative initiatives agreed so far](#)

[Press release: EU negotiators agree on strengthening Europe's cybersecurity](#)

[Press release: Joint Communication 'EU-China – A Strategic Outlook'](#)

IP/19/1832

Press contacts:

[Nathalie VANDYSTADT](#) (+32 2 296 70 83)

[Marietta GRAMMENOU](#) (+32 2 298 35 83)

General public inquiries: [Europe Direct](#) by phone [00 800 67 89 10 11](#) or by [email](#)