REPLIES OF THE EUROPEAN COMMISSION TO THE EUROPEAN COURT OF AUDITORS SPECIAL REPORT: "5G ROLL-OUT IN THE EU: DELAYS IN DEPLOYMENT OF NETWORKS WITH SECURITY ISSUES REMAINING UNRESOLVED"

EXECUTIVE SUMMARY

Commission's introductory remarks

I. Deploying 5G networks in a swift and secure manner is a major priority for the European Commission. Protecting 5G networks against cyber threats is about assessing and mitigating threats and risks. Those threats and risks have been identified and assessed jointly by Member States, with the support of the Commission and ENISA, and on this basis, a set of comprehensive measures have been identified to mitigate those risks. While work is still ongoing in some Member States, a vast majority of Member States have already reinforced or are in the process of reinforcing security requirements for 5G networks based on the EU Toolbox.

The EU Toolbox has been recognised as a comprehensive framework for addressing 5G security risks.

The coordinated action on 5G cybersecurity at EU-level and the EU Toolbox fit into a broader European framework for the protection of electronic communications networks and other critical infrastructures, and complements existing measures such as the European Electronic Communications Code, the Telecoms Framework, the Cybersecurity Act, and the Directive on security of network, information systems (NIS Directive) and, as the case may be, the free movement rules laid down in the Treaty and the Charter of fundamental rights of the EU.

III. 5G will play a key role in our digital economy and society in the years to come. We need to ensure that 5G networks are cybersecure and resilient against increasing cyber threats and incidents. That is why the Commission and Member States have put in place a coordination process aimed at defining and implementing a comprehensive 5G security framework, in the form of a Toolbox of risk mitigation measures agreed in January 2020, in order to address effectively major risks to 5G networks, such as criminal hacking, espionage and sabotage, in a coordinated way. While work is still ongoing in some Member States, a vast majority of Member States have already reinforced or are in the process of reinforcing security requirements for 5G networks based on the EU Toolbox.

VII. The EU Toolbox provides a framework for promoting consistency in the internal market, while respecting national security competences in this area.

Regarding Member States' approach to high-risk vendors, the Commission considers that it will only be possible to make a conclusive assessment, when more information is available.

While implementation is underway, the Commission is working with Member States in the NIS Cooperation Group to promote alignment and convergence among national approaches.

IX. First indent- The Commission accepts the recommendation.

Second indent - The Commission accepts the recommendation.

Third indent - The Commission accepts the recommendation.

The Commission will carry out the assessment taking into account national competences.

INTRODUCTION

04. The Commission acknowledges the existence of 5G security risks, however it points out that 5G networks technology and standards can also bring security improvements compared with previous network generations.

OBSERVATIONS

30. While 4G can already address a wide range of services, 5G should constitute a "frog leap", a major change compared to 4G, so the main challenge is the transition from 4G to 5G, deploying 5G across the whole EU. The risk for a digital gap always exists but it is planned to address this risk as a policy priority in the Policy Programme on the Path to the Digital Decade in relation to the trajectories to the 5G target of 100% coverage of all populated areas by 2030 and thereby supporting Member States to take action in this area, especially with regard access in rural areas.

32. The 5G observatory has been a reliable source to monitor 5G deployment in EU and beyond, even though some shortcomings occurred. Commission services expect to have more up-to-date information available with the new Contractor.

Common Commission reply to paragraphs 48 and 49:

The Commission considers the choice of instrument (Recommendation) and the collaborative approach with Member States to identify risks and mitigating measures as the most appropriate course of action to address 5G security risks in a swift, effective and concerted manner.

The Commission opted for a Recommendation and for working collaboratively with Member States for the identification of risks and mitigation measures in view of the complexity and the cross-cutting nature of the subject matter across national and EU competences and the significant national security dimension. In addition, the Commission also took into account the fact that Member States have very different national contexts (market structure, cybersecurity capabilities, threat intelligence, etc.).

The EU Toolbox represents a nimble risk-based instrument to address security challenges, which allowed to handle 5G cybersecurity aspects in a timely and efficient manner.

In its Communication 'Secure 5G deployment in the EU - Implementing the EU Toolbox' from January 2020, the Commission announced that it would provide support for the implementation of Toolbox measures relating to security requirements, notably with regard to relevant provisions under European rules on electronic communications, and consider the added value of possible implementing acts detailing technical and organisational security measures in order to complement national rules and enhance the effectiveness and consistency of security measures imposed on the operators.

Common Commission reply to paragraphs 51 and 52:

In the context of the review of the Commission Recommendation which took place in December 2020, the Commission interviewed competent authorities of all Member States. They qualified Europe's coordinated action on 5G cybersecurity as timely, effective and proportionate. The collaborative approach between national authorities, the Commission, ENISA and other relevant stakeholders was considered suitable to address this complex issue. It allowed the timely definition of common objectives and methodologies, while allowing Member States to adapt measures to their national circumstances.

The EU Toolbox and the Progress report published by the NIS Cooperation Group in July 2020 recommend to define implementation plans and/or transition periods for those operators currently using equipment of high-risk suppliers or having already entered into contracts with high-risk suppliers before the adoption of the EU Toolbox (e.g. by taking into account equipment upgrade cycles, in particular the migration from 'non stand-alone' to 'stand-alone' 5G networks).

55. The Commission takes note of the observations reported by the European Court of Auditors.

To further support their implementation, the Toolbox criteria for assessing high-risk vendors have been subject to numerous exchanges among competent national authorities within the NIS Cooperation Group, since the EU Toolbox was agreed.

56. The EU Toolbox recommends to take into account the risk factors presented in the EU Coordinated risk assessment as well as country-specific information (e.g. threat assessment from national security services, etc.) for the assessment of the risk profile of suppliers.

61. The supplier's ability to assure supply is one of the criteria recommended by the EU Toolbox to assess the risk profile of suppliers. The ability to assure supply could also be affected by possible trade sanctions faced by a particular vendor, as mentioned in the risk scenario on 'Dependency' in the EU Coordinated risk assessment.

Common Commission reply to paragraphs 70 and 73:

The Commission and Member States are sharing detailed information on the Toolbox implementation at national level within the NIS Cooperation Group. As regards public disclosure of non-public information, this is the responsibility of Member States.

Common Commission reply to paragraphs 74 to 76 and Box 5:

The EU Toolbox provides a framework for promoting consistency in the internal market, while respecting national security competences in this area.

Regarding Member States' approach to high-risk vendors, the Commission considers that it will only be possible to make a conclusive assessment, when more information is available.

While implementation is underway, the Commission is working with Member States in the NIS Cooperation Group to promote alignment and convergence among national approaches.

CONCLUSIONS AND RECOMMENDATIONS

81. Deploying 5G networks in a swift and secure manner is a major priority for the Commission. Protecting 5G networks against cyber threats is about assessing and mitigating threats and risks. Those threats and risks have been identified and assessed jointly by Member States, with the support of the Commission and ENISA, and on this basis, a set of comprehensive measures have been identified to mitigate those risks. While work is still ongoing in some Member States, a vast majority of Member States have already reinforced or are in the process of reinforcing security requirements for 5G networks based on the EU Toolbox.

The EU Toolbox provides a comprehensive framework for addressing 5G security risks.

83. 5G constitutes a "frog leap", a major change compared to 4G, so the main challenge to avoid the digital divide is the transition from 4G to 5G across the whole EU.

5G specifications cover a whole range of performances indicators, notably related to vertical use cases. This may involve, among others, reliability requirements, speed of service instantiation, flexibility of implementation, security levels.

Recommendation 1 – Promote the even and timely deployment of 5G networks within the EU

a) The Commission accepts the recommendation.

The Commission shall work together with Member States towards developing a common definition of the expected quality of service of 5G networks. In the context of the Digital Decade and the proposed decision on the 2030 Digital Policy Programme, the Commission intends to work with Member States on a common approach to 5G service quality in the EU including for the comparability of measurements and monitoring data.

Quality of service does not involve only speed and latency, but covers a whole range of performance indicators, notably related to vertical use cases.

The Commission intends to work together with Member States to define such measurements as well as to carry yearly checkpoints and recommend policies, measures and actions to achieve full 5G coverage by 2030.

The Digital Policy Programme will set up a robust governance through a monitoring and cooperation mechanism to ensure progress towards the fulfilment of the Policy Programme objectives, including 5G deployment, and recommend Member States' remedial action in this respect.

b) The Commission accepts the recommendation.

c) The Commission accepts the recommendation.

Recommendation 2 – Foster a concerted approach to 5G security among Member States

a) The Commission accepts the recommendation.

The Commission will assess, together with Member States, the need for further action or support, for instance in the form of guidance related to certain aspects of the EU Toolbox.

b) The Commission accepts the recommendation.

The monitoring and reporting exercise will be done by the Commission, in full collaboration with Member States and ENISA.

c) The Commission accepts the recommendation.

Recommendation 3 – Monitor Member State approaches towards 5G security and assess the impact of divergences on the effective functioning of the single market

a) The Commission accepts the recommendation.

b) The Commission accepts the recommendation.

The Commission will carry out the assessment taking into account national competences.

Under the EU Toolbox, it is for Member States to decide on the exact scope of the appropriate restrictions and/or necessary exclusions for key assets defined as critical and sensitive in the EU Coordinated risk assessment (e.g. core network functions, network management and orchestration functions, and access network functions), to effectively mitigate identified risks, also taking into account the threat assessment by national intelligence services. Member States have the right to take measures related to national security, including potential restrictions or exclusions of high-risk vendors.