EUROPEAN
COMMISSION

Brussels, 15.6.2023
C(2023) 4049 final

COMMUNICATION FROM THE COMMISSION

Implementation of the 5G cybersecurity Toolbox

COMMUNICATION FROM THE COMMISSION

Implementation of the 5G cybersecurity Toolbox

The security of 5G networks is a major priority for the European Commission. Those networks are a central infrastructure, providing the foundation for a wide range of services essential for the functioning of the internal market and the maintenance and operation of vital societal and economic functions. To protect 5G networks, cyber threats and risks have been identified and assessed jointly[1] by Member States, with the support of the Commission and the EU Cybersecurity Agency (ENISA), and on this basis, a set of comprehensive measures have been identified to mitigate those risks, in the form of the EU Toolbox on 5G Cybersecurity[2] adopted in 2020 by the NIS Cooperation Group and endorsed by the European Council and the Commission.

At Versailles in March 2022, the Heads of State or Government decided to take more responsibility for our security and to take further decisive steps towards building our European sovereignty, and reducing our dependencies, including by strengthening our cyber-resilience and protecting our infrastructure – particularly our critical infrastructure[3]. The implementation of the EU Toolbox is an essential component of the Security Union Strategy[4] and supports the broader European policy framework of strategic autonomy and enhanced resilience, and the specific framework for the protection of electronic communications networks and other critical infrastructures[5], in particular the implementation of Article 40 of the European Electronic Communications Code, which requires '*that operators take appropriate and proportionate technical and organisational measures to appropriately manage the risks posed to the security of networks and services*'[6].

Under the EU Toolbox, given the ultimate objective to ensure the security and resilience of the 5G networks and their sustainability, Member States agreed on the need to assess the risk profile of individual suppliers and, as a consequence to apply relevant restrictions for suppliers considered to be high risk, including necessary exclusions to effectively mitigate risks, for key assets, as indicated in the toolbox.

According to the EU coordinated risk assessment, the risk profile of individual suppliers can be assessed on the basis of several factors. The likelihood of the supplier being subject to interference from a non-EU country is presented as one of the key aspects in the assessment of non-technical vulnerabilities related to 5G networks, and may be facilitated by several factors, in particular the link between a supplier and a government of a given third country, the third country's legislation, and characteristics of the supplier's corporate ownership.

---

[1] Report on an EU coordinated risk assessment of 5G networks, NIS Cooperation Group

[2] EU Toolbox on 5G Cybersecurity, NIS Cooperation Group, 29 January 2020. The EU Toolbox was adopted by the Member States' national cybersecurity authorities and endorsed by the European Council and the Commission.

[3] Informal meeting of the Heads of State or Government, Versailles declaration, 10-11 March 2022.

[4] EU Security Union Strategy, COM(2020) 605 final

[5] EU Toolbox on 5G Cybersecurity, NIS Cooperation Group, 29 January 2020. The EU Toolbox was adopted by the Member States' national cybersecurity authorities and endorsed by the European Council and the Commission.

[6] This provision is replaced by Article 21(1) of the NIS2 Directive as from October 2024.

The Commission takes note of and welcomes the adoption of the Second Progress report on the implementation of the EU Toolbox by the NIS Cooperation Group.

In light of this report, the Commission is strongly concerned by the risks posed by certain suppliers of mobile network communication equipment to the security of the Union, as reflected also by decisions taken by some Member States. The NIS Report highlights the 'clear risk of persisting dependency on high-risk suppliers in the internal market with potentially serious negative impacts on security for users and companies across the EU and the EU's critical infrastructure'.

As mentioned in the NIS Progress Report and in an earlier report by the European Court of Auditors[7], it is evident that 5G suppliers exhibit clear differences in their characteristics, in particular as regards their likelihood of being influenced by specific third countries which have security laws and corporate governance that are a potential risk for the security of the Union. As also indicated in the NIS report, Huawei and ZTE have been subject to public decisions and advice in certain Member States[8], based on national security concerns, including assessments by those Member States' intelligence services. In other Member States, decisions to restrict or exclude certain suppliers from their 5G networks have been made confidentially, based on their assessment. The findings of those Member States are similar to the analysis of the competent authorities of certain third countries[9].

Due to these high risks, and based on an assessment of the criteria set out in the Toolbox for identifying 'high-risk suppliers', the Commission considers that decisions adopted by Member States to restrict or exclude Huawei and ZTE are justified and compliant with the 5G Toolbox. Without prejudice to the Member States' competences as regards national security, the Commission has also applied the Toolbox criteria to assess the needs and vulnerabilities of its own corporate communications systems and those of the other European institutions, bodies and agencies, as well as the implementation of Union funding programmes in the light of the Union's overall policy objectives.

In this context, consistently with certain Member States' application of the 5G Toolbox, the Commission considers, that Huawei and ZTE represent in fact materially higher risks than other 5G suppliers. This assessment by the Commission, in the light of the Toolbox criteria, is based on the available information on:

1) national assessments of EU Member States and third countries in relation to risks posed by suppliers
2) relevant legislative and regulatory texts of EU Member States and third countries related to measures addressing risks from suppliers;
3) relevant report of the European Court of Auditors;
4) the likelihood of interference by the government of a non-EU country without adequate legal or judicial constraints;
5) the level of malicious activities affecting the cybersecurity of the EU institutions;
6) the risks of potential disruption affecting the supply chain of 5G equipment in the current geopolitical context;

[7] Special report: security of 5G networks (europa.eu)
[8] Second Progress Report on the implementation of the EU Toolbox on 5G Cybersecurity, 15 June 2023
[9] Huawei Designated Vendor Direction (publishing.service.gov.uk)

7) the significant presence of these suppliers in the EU's 5G networks.

Ten Member States have used their powers to impose obligations to restrict or exclude high-risk suppliers from their 5G networks. In light of the interconnected character of networks, the Commission urges Member States that have not yet implemented the Toolbox, to adopt urgently relevant measures as recommended in the EU Toolbox, in order to effectively and quickly address the risks, taking into account what other Member States have already done in line with the Toolbox as well as this assessment.

They shall also act considering the risks related to potential disruptions affecting the supply chain of 5G equipment, in light of the current geopolitical context – and the significant presence of those suppliers across the EU's 5G networks, which is creating strong vulnerabilities and a dependency for the Union as a whole.

When implementing these measures, the Commission urges Member States to also take utmost account of the recommendations in the NIS report, in particular regarding the scope of restrictions, which should cover critical and highly sensitive assets identified in the EU Coordinated risk assessment, including the Radio Access Network, and regarding the use of transition periods, which shall be defined to ensure the removal of equipment in place within the shortest possible timeframe.

The Commission may take further initiatives to support the comprehensive implementation of the 5G Toolbox.

Additionally, as mentioned above, the Commission is also concerned about the security and confidentiality of the Commission's corporate communications and of those of other EU institutions, bodies and agencies. As part of its corporate cybersecurity policy, and in application of the 5G cybersecurity toolbox, the Commission will take measures to avoid exposure of its corporate communications to mobile networks using Huawei and ZTE as suppliers. These measures will include not procuring new connectivity services, that rely on equipment from those suppliers in application of relevant security conditions. The Commission will work with Member states and telecom operators to make sure that those suppliers are progressively phased out from existing connectivity services of the Commission sites.

This will apply to all Commission sites, including its main seats, its Representations and offices in all Member States[10]. The Commission will encourage other EU institutions, bodies and agencies to take similar measure. The Commission will take the necessary steps to swiftly implement these decisions.

The Commission also intends to reflect this decision, in accordance with its competences under the respective governance rules, in all relevant EU funding programmes and instruments.

[10] Including its executive agencies.