European Commission - Press release

Commission announces next steps on cybersecurity of 5G networks in complement to latest progress report by Member States*

Brussels, 15 June 2023

Today, EU Member States, with the support of the European Commission and ENISA, the EU Agency for Cybersecurity, published a second **progress report** on the implementation of the EU Toolbox on 5G cybersecurity. The report also addresses some of the recommendations of the European Court of Auditors' Special Report of January 2022. In complement to the progress report, the Commission today adopted a **Communication** on the implementation of the toolbox by Member States and in the EU's own corporate communications and funding activities.

As regards strategic measures and in particular enacting restrictions **on high-risk suppliers**, the progress report records that 24 Member States have adopted or are preparing legislative measures giving national authorities the powers to perform an assessment of suppliers and issue restrictions. Out of them, 10 Member States have imposed such restrictions and 3 Member States are currently working on the implementation of the relevant national legislation. Given the importance of the connectivity infrastructure for the digital economy and dependence of many critical services on 5G networks, **Member States should achieve the implementation of the Toolbox without delay**.

The Commission underlines in its Communication its strong concerns about the risks posed by certain suppliers of mobile network communication equipment to the security of the Union. The Commission considers that **decisions adopted by Member States to restrict or exclude Huawei and ZTE from 5G networks are justified and compliant with the 5G Toolbox**. Consistently with such decisions, and on the basis of a broad range of available information, the Commission considers that Huawei and ZTE represent in fact materially higher risks than other 5G suppliers.

Commission Communication on Toolbox implementation

The security of 5G networks is a major priority for the Commission and an essential component of its Security Union Strategy, as 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. The issue is central to the Union's sovereignty, strategic autonomy, and resilience. In its Communication adopted today, 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.

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. Drawing on its own assessment, which is consistent with that of certain Member States, the Commission urges Member States that have not yet implemented the Toolbox, to **adopt urgently relevant measures as recommended in the EU Toolbox**, to effectively and quickly address the risks posed by the identified suppliers.

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**. It will take relevant security measures so as not to procure new connectivity services that rely on equipment from those suppliers, and 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.

The Commission also intends to **reflect this decision in all relevant EU funding programmes and instruments**.

Second progress report on the 5G Toolbox

The report, adopted by Member States, records that further progress was made in the implementation of the **key measures** of the EU Toolbox since the first Progress Report of July 2020.

A vast majority of Member States have reinforced or are in the process of reinforcing security requirements for 5G networks based on the EU Toolbox. However, despite the progress made, the report finds that this situation creates a 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.

The report includes **recommendations for** Member States to:

- Ensure they have **comprehensive and detailed information** from **mobile operators** about the 5G equipment currently deployed and about their plans for deploying or sourcing new equipment.
- In **assessing the risk profile of suppliers**, Member States should consider the objective criteria recommended in the EU Toolbox. In this context, 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. Furthermore, **designations made by other Member States** concerning high-risk suppliers should be taken into account, with a view to promote consistency and a high level of security across the Union.
- Based on the assessment of suppliers, **Member States should impose restrictions on high-risk suppliers without delay**, i.e. considering that a loss of time can increase vulnerability of networks in the Union and the Union's dependency on high-risk suppliers, especially for Member States with a high presence of potential high-risk suppliers.
- To effectively mitigate risks, Member States should ensure that the **restrictions cover critical and highly sensitive assets** identified in the EU Coordinated risk assessment, **including the Radio Access Network**.
- For types of equipment covered by the restrictions, operators **should not be allowed to install new equipment.** If transition periods are allowed for the removal of existing equipment, they shall be defined to ensure the **removal of equipment in place within the shortest possible timeframe**, taking into account the security risk of keeping equipment from high-risk suppliers in place, and should not be applied to allow the continued deployment of new equipment from high-risk suppliers.
- Implement **restrictions for Managed Service Providers** (MSPs), and in case functions are outsourced to MSPs, impose enhanced security provisions around the access that MSPs are given.
- Further discuss the **applicability of measures related to diversification of suppliers**, and how to best ensure that any potential diversification does not result in new or increased security risks but contributes to security and resilience.
- **Enforce technical measures** and ensure a **strong level of supervision**. Particular attention should be given to certain measures, notably ensuring the application of baseline security requirements, raising security standards in suppliers' processes through robust procurement condition and ensuring secure 5G network management, operation and monitoring.

Background

The EU Toolbox on 5G cybersecurity (EU Toolbox) published in January 2020 by Member States' authorities (NIS Cooperation Group), with the support of the Commission and ENISA, aims to address risks related to the cybersecurity of 5G networks. It identifies and describes a set of strategic and technical measures, as well as corresponding supporting actions to reinforce their effectiveness, which may be put in place to mitigate the risks identified in the report on an EU coordinated risk assessment of 5G cybersecurity, which was based on national risk assessments.

The Toolbox and its key recommendations have been endorsed by the Commission and Member States at the highest level. In October 2020, the European Council called on the EU and the Member States "to make full use of the 5G cybersecurity Toolbox adopted on 29 January 2020, and in particular to apply the relevant restrictions on high-risk suppliers for key assets defined as critical and sensitive in the EU coordinated risk assessment, based on common objective criteria". In its Recommendation of December 2022, the Council of the EU reiterated that "it is important that the Member States achieve the implementation of the measures recommended in the EU Toolbox on 5G cybersecurity and in particular that the Member States enact restrictions on high-risk suppliers, considering that a loss of time can increase vulnerability of networks in the Union".

A first report on Member States' progress in implementing the EU Toolbox was published in July 2020. It concluded that concrete steps had been taken to implement the EU Toolbox. Many Member States had already adopted or were well advanced in the preparation of more advanced security

measures on 5G cybersecurity. In its Special Report of January 2022, the Court of Auditors concluded that progress has been made to reinforce the security of 5G networks since the EU Toolbox was adopted. However, the Court also highlighted that Member States applied divergent approaches regarding the use of equipment from high-risk suppliers or the scope of the restrictions.

For More Information

Commission Communication on implementation of 5G cybersecurity toolbox

Second progress report on the EU 5G cybersecurity toolbox

EU Cybersecurity Policies

EU 5G Toolbox

**Updated on 15/06/2023*

IP/23/3309

Quotes:

We need further urgent actions under the EU toolbox. In particular to adopt the necessary restrictions for high-risk suppliers, in order to ensure the security of the Union's critical infrastructure. While some Member States have made progress today's report show that we are not yet where we need to be. The Commission is doing the necessary to ensure security in its own networks and funding instruments.
Margrethe Vestager, Executive Vice-President for a Europe Fit for the Digital Age - 15/06/2023

This report makes clear that it is an urgent priority that national authorities complete their efforts to fully implement the EU's 5G Toolbox measures in order to protect the EU's collective security. Completing these efforts, and in particular identifying and restricting access to high-risk 5G suppliers, is vital for sealing the Security Union's infrastructure.
Margaritis Schinas, Vice-President for Promoting our European Way of Life - 15/06/2023

We have been able to reduce or eliminate our dependencies in other sectors such as energy in record time, when many thought it was impossible. The situation with 5G should be no different: we can't afford to maintain critical dependencies that could become a "weapon" against our interests. That would be too critical a vulnerability and a serious risk to our common security. I therefore call on all Member States and telecom operators to take the necessary measures without further delay.
Thierry Breton, Commissioner for Internal Market - 15/06/2023

Press contacts:

Johannes BAHRKE (+32 2 295 86 15)
Marietta GRAMMENOU (+32 2 298 35 83)

General public inquiries: Europe Direct by phone 00 800 67 89 10 11 or by email