

(English version)

**Question for written answer E-003145/25
to the Commission
Dolors Montserrat (PPE)
(30 July 2025)**

Subject: Risks to judicial security and the integrity of intelligence cooperation due to the use of Huawei technology

The Spanish Government has awarded Huawei a public contract to provide storage for SITEL (Integrated Telecommunications Interception System), which hosts court-authorised wiretaps. This has been cause for concern in the US because of the danger of this information ending up in the hands of the Chinese Communist regime. Back in 2020, the Commission warned about the risk posed by some technology suppliers classed as ‘high-risk’, such as Huawei.

Given that SITEL manages highly sensitive information related to judicial investigations, international police cooperation and national security:

1. Does the Commission consider this type of contract to breach the guidelines laid out in the EU toolbox for 5G security as regards barring high-risk suppliers from critical roles, even outside the realm of 5G networks?
2. Does the Commission intend to propose a binding framework that extends the principles established in this toolbox to other critical technology sectors, such as the judicial and intelligence systems?
3. Does the Commission consider decisions like Spain’s to compromise the country’s reliability as a partner in intelligence and security cooperation, at both European and international levels?

Submitted: 30.7.2025

**Answer given by Executive Vice-President Virkkunen on behalf of the European Commission
(17 November 2025)**

In the communication on the implementation of the EU 5G cybersecurity toolbox of 15 June 2023 ⁽¹⁾, the Commission assessed that Huawei (and ZTE) present materially higher risks than other 5G suppliers and committed to avoid exposure of its own corporate communications networks to mobile networks using Huawei and ZTE as suppliers and to reflect this decision, in accordance with its competences under the respective governance rules, in all relevant EU funding programmes and instruments.

The Commission also considered that decisions adopted by the Member States to restrict or exclude Huawei and ZTE are justified and compliant with the 5G toolbox. It urged all Member States to implement the 5G toolbox and take measures to mitigate the risks linked to these suppliers.

The contract concluded by the Spanish Ministry of the Interior with Huawei can potentially create a dependency on a high-risk supplier in a critical and sensitive sector that would increase the risk of foreign interference.

In line with the 5G toolbox and as announced in the ProtectEU Strategy ⁽²⁾ of April 2025, the Commission will look more broadly at the security and resilience of information and communication technology (ICT) supply chains and infrastructure in the upcoming revision of the Cybersecurity Act, with a view to avoid critical dependencies and de-risk our ICT supply chains from high-risk suppliers.

⁽¹⁾ C(2023) 4049 final.
⁽²⁾ COM(2025) 148 final.