Criteria for defining a high-risk equipment manufacturer

The criteria for defining a high-risk equipment manufacturer implement the EU 5G Toolbox strategic measure (SM03): "Assessing the risk profile of suppliers and applying restrictions for suppliers considered to be high risks – including necessary exclusions to effectively mitigate risks – for key assets".

This set of criteria supports section 244a of the currently applicable Act on Electronic Communications Services, which regulates the equipment used in critical parts of communications networks. The purpose of the provision is to ensure that equipment used in critical parts of communications networks does not endanger national security or national defence. Any assessment of endangerment of national security or national defence is based on evaluations carried out by the authorities responsible for internal affairs, foreign affairs and defence. The criteria for high-risk equipment manufacturers support such assessments.

In cooperation between the security authorities (Traficom, the Finnish Defence Forces and the Finnish Security and Intelligence Service), it has been assessed that, in Finland, operators may be considered high-risk equipment manufacturers if they meet one or more of the following criteria, which have also been identified in the EU-wide coordinated risk assessment and by Finland's key reference countries:

- Risk related to the equipment manufacturer's country of origin and regulatory environment:
  - The legislation of the equipment manufacturer's country of origin, that is, a third country outside the NATO, EU or EEA area, or of the country where the company has its main establishment, does not comply with the legal and democratic principles adopted in the EU, and information security and data protection legislation cannot be applied in that country on principles equivalent to those applied in the EU.
  - Due to the regulatory framework in force in the equipment manufacturer's country of origin, it is not possible to apply security, information security, data protection or disclosure agreements in that country.
  - The equipment manufacturer, including its personnel, may be subject to pressure by such a third country or exposed to external influence.
  - The equipment manufacturer, including its ownership structure, has close links to the governments, authorities or state-owned enterprises of such third countries (non-EU countries).
- Risk of hostile cyber activities or actions endangering national security against Finland or its allies:
  - The equipment manufacturer has close links to states or organisations that carry out hostile cyber activities, information influence operations or other actions that endanger national security against Finland or its allies.
- Risk related to the equipment manufacturer's security of supply and supply chain:
  - The equipment manufacturer's ability to deliver equipment or services that meet applicable standards in changing operating environments.
  - The transparency of the equipment manufacturer's cybersecurity practices and its track record in remedying known vulnerabilities and defects.
  - The equipment manufacturer's ability and willingness to manage risks related to its supply chain or logistics chain in changing operating environments, together with its subcontractors.

In addition to the criteria mentioned above, other criteria may also be applied when identifying a high-risk equipment manufacturer, particularly when assessing the endangerment of national security outside the context of communications network security.